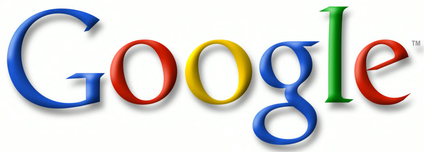


This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

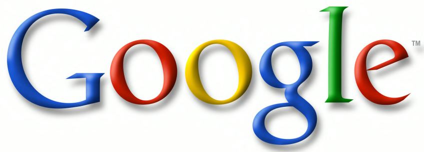
+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at http://books.google.com/



Over dit boek

Dit is een digitale kopie van een boek dat al generaties lang op bibliotheekplanken heeft gestaan, maar nu zorgvuldig is gescand door Google. Dat doen we omdat we alle boeken ter wereld online beschikbaar willen maken.

Dit boek is zo oud dat het auteursrecht erop is verlopen, zodat het boek nu deel uitmaakt van het publieke domein. Een boek dat tot het publieke domein behoort, is een boek dat nooit onder het auteursrecht is gevallen, of waarvan de wettelijke auteursrechttermijn is verlopen. Het kan per land verschillen of een boek tot het publieke domein behoort. Boeken in het publieke domein zijn een stem uit het verleden. Ze vormen een bron van geschiedenis, cultuur en kennis die anders moeilijk te verkrijgen zou zijn.

Aantekeningen, opmerkingen en andere kanttekeningen die in het origineel stonden, worden weergegeven in dit bestand, als herinnering aan de lange reis die het boek heeft gemaakt van uitgever naar bibliotheek, en uiteindelijk naar u.

Richtlijnen voor gebruik

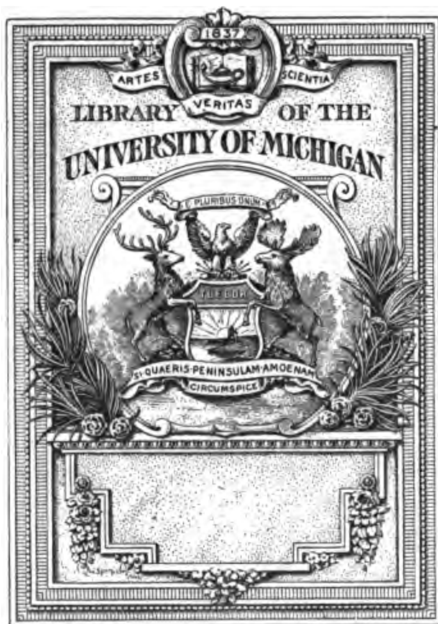
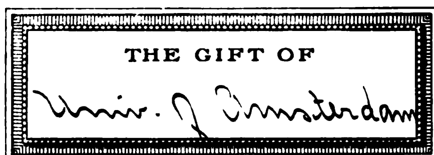
Google werkt samen met bibliotheken om materiaal uit het publieke domein te digitaliseren, zodat het voor iedereen beschikbaar wordt. Boeken uit het publieke domein behoren toe aan het publiek; wij bewaren ze alleen. Dit is echter een kostbaar proces. Om deze dienst te kunnen blijven leveren, hebben we maatregelen genomen om misbruik door commerciële partijen te voorkomen, zoals het plaatsen van technische beperkingen op automatisch zoeken.

Verder vragen we u het volgende:

+ *Gebruik de bestanden alleen voor niet-commerciële doeleinden* We hebben Zoeken naar boeken met Google ontworpen voor gebruik door individuen. We vragen u deze bestanden alleen te gebruiken voor persoonlijke en niet-commerciële doeleinden.
+ *Voer geen geautomatiseerde zoekopdrachten uit* Stuur geen geautomatiseerde zoekopdrachten naar het systeem van Google. Als u onderzoek doet naar computervertalingen, optische tekenherkenning of andere wetenschapsgebieden waarbij u toegang nodig heeft tot grote hoeveelheden tekst, kunt u contact met ons opnemen. We raden u aan hiervoor materiaal uit het publieke domein te gebruiken, en kunnen u misschien hiermee van dienst zijn.
+ *Laat de eigendomsverklaring staan* Het "watermerk" van Google dat u onder aan elk bestand ziet, dient om mensen informatie over het project te geven, en ze te helpen extra materiaal te vinden met Zoeken naar boeken met Google. Verwijder dit watermerk niet.
+ *Houd u aan de wet* Wat u ook doet, houd er rekening mee dat u er zelf verantwoordelijk voor bent dat alles wat u doet legaal is. U kunt er niet van uitgaan dat wanneer een werk beschikbaar lijkt te zijn voor het publieke domein in de Verenigde Staten, het ook publiek domein is voor gebruikers in andere landen. Of er nog auteursrecht op een boek rust, verschilt per land. We kunnen u niet vertellen wat u in uw geval met een bepaald boek mag doen. Neem niet zomaar aan dat u een boek overal ter wereld op allerlei manieren kunt gebruiken, wanneer het eenmaal in Zoeken naar boeken met Google staat. De wettelijke aansprakelijkheid voor auteursrechten is behoorlijk streng.

Informatie over Zoeken naar boeken met Google

Het doel van Google is om alle informatie wereldwijd toegankelijk en bruikbaar te maken. Zoeken naar boeken met Google helpt lezers boeken uit allerlei landen te ontdekken, en helpt auteurs en uitgevers om een nieuw leespubliek te bereiken. U kunt de volledige tekst van dit boek doorzoeken op het web via `http://books.google.com`


1837
ARTES
SCIENTIA
VERITAS
LIBRARY OF THE
UNIVERSITY OF MICHIGAN
E PLURIBUS UNUM
TUEBOR
SI QUAERIS PENINSULAM AMOENAM
CIRCUMSPICE

THE GIFT OF
Univ. of Amsterdam

Mathematics
QA
171
.C67

INLEIDING TOT DE THEORIE VAN GALOIS EN DE THEORIE DER SUBSTITUTIEGROEPEN.

INLEIDING TOT DE THEORIE VAN GALOIS

EN DE

THEORIE DER SUBSTITUTIEGROEPEN.

ACADEMISCH PROEFSCHRIFT

TER VERKRIJGING VAN DEN GRAAD VAN

DOCTOR IN DE WIS- EN NATUURKUNDE,

AAN DE UNIVERSITEIT VAN AMSTERDAM,

OP GEZAG VAN DEN RECTOR-MAGNIFICUS

Mr. D. JOSEPHUS JITTA,

hoogleeraar in de faculteit der rechtsgeleerdheid,

IN HET OPENBAAR TE VERDEDIGEN

op Dinsdag 4 December 1900,

des namiddags te 3 uur,

in de Aula der Universiteit,

DOOR

DERK ÇOELINGH,

geboren te Deventer.

AMSTERDAM. — J. H. & G. VAN HETEREN.
1900.

Aan mijne Moeder

en

mijne aanstaande Vrouw.

157020

Het is mij eene aangename taak hier mijn dank te betuigen aan alle Hoogleeraren in de faculteit der Wis- en Natuurkunde, die tot mijne opleiding hebben medegewerkt, in het bijzonder aan mijnen hooggeachten Promotor Prof. Dr. D. J. KORTEWEG *en aan de Hoogleeraren* Prof. Dr. J. D. VAN DER WAALS *en* Prof. Dr. A. J. VAN PESCH.

INHOUD.

LIJST VAN TECHNISCHE UITDRUKKINGEN. [1]

[1] De getallen wijzen de bladzijden aan, waarop de bepalingen dezer uitdrukkingen te vinden zijn.

HOOFDSTUK I.

INLEIDING. — GESCHIEDKUNDIG OVERZICHT.

§ 1. De oplossing der vierkantsvergelijkingen is in meetkundigen vorm reeds bij EUCLIDES te vinden: de verdeeling eener lijn in de uiterste en middelste reden (Eucl. II, 11) komt toch neer op de oplossing van de vierkantsvergelijking

$$x^2 = a(a - x)$$

en de constructies:

„in een gegeven driehoek een parallelogram van gege-„ven oppervlakte te beschrijven, dat met den driehoek „een hoek gemeen heeft" (VI, 28) en „aan een gegeven „driehoek een parallelogram van gegeven oppervlakte te „beschrijven, dat met den driehoek een buitenhoek ge-„meen heeft" (VI, 29) geven [1]) de meetkundige oplossing van de vierkantsvergelijkingen

$$x(a - x) = b^2 \text{ en } x(a + x) = b^2.$$

HERON VAN ALEXANDRIË (100 v. Chr.) heeft de algemeene vierkantsvergelijking reeds algebraïsch behandeld [2]): hij vindt voor de middellijn d van een cirkel, waarvoor

---

[1]) Deze opmerking is van MATTHIESSEN. Zie CANTOR. Vorlesungen über Geschichte der Mathematik I, Kapitel 12.

[2]) CANTOR. Kapitel 19.

de som van de oppervlakte, den omtrek en die middellijn zelve gelijk S gegeven is

$$d = \frac{1}{11}\left(\sqrt{154\,S + 841} - 29\right)$$

hetgeen niet anders is dan de oplossing van de vierkantsvergelijking

$$\frac{1}{4}\pi d^2 + \pi d + d = S$$

als men $\pi = \frac{22}{7}$ stelt.

Diophantos, ± 300 n. Chr. (?), geeft ook de bekende oplossing der vierkantsvergelijking, maar verklaart die onmogelijk, als niet de tweedemacht van de halve coefficient der onbekende verminderd met den bekenden term een kwadraatgetal is [1]).

Ook bij de Indiërs vindt men de oplossing der vierkantsvergelijkingen; zij hebben die van de Grieken overgenomen. Het onderscheid tusschen de verschillende vormen der vergelijkingen

$$ax^2 + bx = c \qquad ax^2 = bx + c \qquad ax^2 + c = bx$$

vervalt bij hen, omdat zij ook met negatieve getallen rekenen. Ook komen bij hen en bij de Arabieren de *twee* wortels eener vierkantsvergelijking te voorschijn [2]).

§ 2. Wat de derde-machtsvergelijkingen betreft, Archimedes, 287—212 v. Chr., komt er het eerste op, door het vraagstuk: een bol zóo door een vlak te snijden, dat de inhouden der beide stukken eene gegeven verhouding hebben. Hij beweert [3]) dat de vergelijking

$$x^3 - ax^2 + \frac{4}{9}a^2 b = 0$$

oplosbaar is, d. w. z. een positieven wortel heeft, zoolang

[1]) Cantor. Kapitel 23. [2]) Cantor Kapitel 33.
[3]) Cantor. Capitel 14.

$b < \frac{1}{3} a$ is. Zijn bewijs voor de juistheid dezer bewering is echter verloren gegaan.

Ook DIOPHANTOS komt tot eene derdemachtsvergelijking

$$x^3 - 3x^2 + 3x - 1 = x^2 + 2x + 3$$

waaruit hij vindt $x = 4$ [1]). Hoe hij tot den wortel van deze ontbindbare vergelijking komt, is echter een raadsel.

De Indiër BHÂSKARA (geboren 1114) lost de vergelijkingen

$$x^3 + 12x = 6x^2 + 35 \text{ en } x^4 - 2(x^2 + 200x) = 9999$$

op door ze te schrijven

$$(x - 2)^3 = 27 \text{ en } (x^2 + 1)^2 = (2x + 100)^2. \text{ [2])}$$

Ook de Arabieren kwamen niet verder met de oplossing der derdemachtsvergelijkingen [3])

LEONARDO VAN PISA geeft (1225?) de oplossing van de vergelijking

$$x^3 + 2x^2 + 10x = 20$$

met eene verbazende nauwkeurigheid: zijne waarde in eene sexagesimale breuk verschilt minder dan $^1/_3$ eenheid van de tiende decimaal van de juiste waarde [4]).

Hoe hij aan deze waarde komt, blijft echter duister.

§ 3. Alle pogingen om de algemeene derdemachtsvergelijking op te lossen waren vergeefsch, totdat in het begin der zestiende eeuw, waarschijnlijk voor het eerst, de Italiaan SCIPIONE DEL FERRO de vergelijking

$$x^3 + ax = b \tag{1}$$

oploste. Eerst in 1545, minstens 30 jaar later, deelde HIERONIMO CARDANO deze oplossing in zijn boek „Ars magna de rebus Algebraicis" mede.

---

[1]) CANTOR. Kapitel 23. [2]) CANTOR. Kapitel 29.
[3]) CANTOR. Kapitel 35. [4]) CANTOR. Kapitel 42.

De twee vergelijkingen

$$u - v = b \quad \text{en} \quad uv = \left(\frac{1}{3}a\right)^3 \qquad (2)$$

behoefden slechts opgelost te worden om voor x te vinden

$$x = \sqrt[3]{u} - \sqrt[3]{v}. \qquad (3)$$

CARDANO bevrijdde ook de algemeene derdemachtsvergelijking van den tweeden term en loste de vergelijking

$$x^3 + ax + b = 0$$

op voor alle teekencombinaties van a en b. Hij vond ook de *drie* wortels der derdemachtsvergelijking en wees op het onherleidbaar geval [1]).

In diezelfde Ars magna geeft CARDANO ook de bekende oplossing van de vierdemachtsvergelijking

$$x^4 + ax^2 + c = bx \qquad (4)$$

zooals die gevonden is door zijn 23-jarigen leerling LUIGI FERRARI [1]). Het eerste lid wordt tot een volkomen vierkant gemaakt:

$$(x^2 + \sqrt{c} + t)^2 = (2\sqrt{c} - a + 2t)\,x^2 + bx + t^2 + 2t\sqrt{c} \qquad (5)$$

vervolgens wordt over de hulpgrootheid t zóo beschikt, dat ook het tweede lid een volkomen vierkant wordt. Daartoe is noodig:

$$t^3 + \left(3\sqrt{c} - \frac{1}{2}a\right)t^2 + \left(2c - a\sqrt{c}\right)t = \frac{1}{8}b^2 \qquad (6)$$

Hieruit is t te vinden. Wordt dan uit beide leden van (5) de wortel getrokken, dan kan x uit eene vierkantsvergelijking bepaald worden.

§ 4. De Fransche wiskundige VIETA (1540—1603) gaf [2]) van de vierdemachtsvergelijking eene eenigszins andere oplossing dan FERRARI. Ook hij verdrijft eerst den twee-

---

[1]) CANTOR. Kapitel 64, 65, 66. [2]) CANTOR. Kapitel 69.

den term, maar hij komt door de invoering van de hulpgrootheid y van

$$x^4 + n x^2 + p x + q = 0 \tag{7}$$

tot $$(x^2 + y)^2 = (2y - n) x^2 - p x + y^2 - q. \tag{8}$$

Het tweede lid wordt een volkomen vierkant als

$$y^3 - \frac{1}{2} n y^2 - q y + \frac{1}{8} (4 n q - p^2) = 0. \tag{9}$$

Een wortel hiervan kan bepaald worden. Verder is dan

$$x^2 + y = \left(x - \frac{p}{2(2y - n)}\right) \sqrt{2y - n} \tag{10}$$

en hieruit wordt x gevonden.

VIETA werd dus geleid tot eene derdemachtsvergelijking, die hij ook eenigszins anders oploste. Hij verdrijft eerst weer den 2den term; vervolgens stelt hij in

$$x^3 + 3 a x = 2 b \tag{11}$$

$$x = \frac{a - y^2}{y}.$$

Daardoor gaat de vergelijking over in

$$y^6 + 2 b y^3 = a^3 \tag{12}$$

die gemakkelijk kan worden opgelost.

§ 5. DESCARTES [1]) geeft in zijne „Géométrie", die 't eerst in 1637 verscheen, eene nieuwe oplossing van de vierdemachtsvergelijking. Deze methode bestaat in 't splitsen van het eerste lid in twee factoren van den 2den graad. VAN SCHOOTEN heeft in zijn bijvoegingen bij 't werk van DESCARTES de methode eenigszins gewijzigd door onbepaalde coefficienten te gebruiken. Hij stelt

$$x^4 - p x^2 - q x + r = (x^2 + y x + z)(x^2 - y x + v) \tag{13}$$

Hij krijgt zoo drie vergelijkingen ter bepaling van y, z en v. Door eliminatie van z en v hieruit vindt hij

---

[1]) CANTOR. Kapitel 76.

$$y^6 - 2py^4 + (p^2 - 4r)y^2 - q^2 = 0 \qquad (14)$$

waaruit y weer te bepalen is. Vervolgens kunnen z en v gemakkelijk gevonden worden en daaruit ook de twee tweedegraadsfactoren van de vierdemachtsvergelijking.

§ 6. De Hollandsche wiskundige JOHANNES HUDDE, vele malen burgemeester van Amsterdam, gaf in 1657 ook eene oplossing [1]) van de kubische vergelijking, die niet zakelijk verschilt van de Italiaansche oplossing. Hij stelt in

$$x^3 + nx + p = 0 \qquad (15)$$

$$x = y + z \qquad (16)$$

waardoor hij vindt

$$y^3 + z^3 + (3yz + n)(y + z) + p = 0 \qquad (17)$$

Hij beschikt nu over y en z zóo, dat

$$3yz = -n \quad \text{en dus} \quad y^3 z^3 = -p \qquad (18)$$

wordt. Uit deze twee vergelijkingen vindt hij door eliminatie van z:

$$y^6 + py^3 - \frac{1}{27}n^3 = 0 \qquad (19)$$

waaruit volgt:

$$y = \sqrt[3]{-\frac{1}{2}p \pm \sqrt{\frac{1}{4}p^2 + \frac{1}{27}n^3}}$$

Zoo vindt hij de formule ook door CARDANO gegeven:

$$x = \sqrt[3]{-\frac{1}{2}p + \sqrt{\frac{1}{4}p^2 + \frac{1}{27}n^3}} + \sqrt[3]{-\frac{1}{2}p - \sqrt{\frac{1}{4}p^2 + \frac{1}{27}n^3}}. \qquad (20)$$

§ 7. Wat de hoogere-machtsvergelijkingen betreft, heeft

[1]) CANTOR. Kapitel 76.

Cardano in een geschrift „De Regula Aliza" dat in 1570 verscheen, behandeld de zesdemachtsvergelijking

$$x^6 + ax^4 + a^2x^2 + a^3 = bx^3. \qquad (21)$$

Hij beschouwt deze vergelijking eerst als ontstaan door de eliminatie van y uit

$$xy = a \quad \text{en} \quad x^3 + y^3 + x^2y + xy^2 = b \qquad (22)$$

Uit deze twee vergelijkingen leidt hij af

$$(x + y)^3 = 2a(x + y) + b \qquad (23)$$

waaruit hij $x + y$ vindt. En nu zijn x en y afzonderlijk gemakkelijk te bepalen [1]).

§ 8. Vieta gaf in 1594 de oplossing van eene vergelijking van den 45sten graad, door van Roomen opgegeven [2]).

Hij ontdekte dat de vergelijking het verband weergaf tusschen de koorde van een boog en de koorde van het 45ste deel van dien boog; hij bracht de oplossing terug tot de oplossing van twee derdemachts- en éene vijfdemachtsvergelijking en hij vond er de 23 wortels van, die hij alleen kon vinden, zoolang men slechts positieve wortels van vergelijkingen toeliet.

§ 9. Tschirnhaus (1651—1708) gaf in de Acta Eruditorum van 1683 eene verhandeling [3]), waarvan de titel „Methodus auferendi omnes terminos intermedios ex data aequatione" meer beloofde dan de inhoud gaf: hij meende in staat te zijn uit elke vergelijking.

$$x^n + a_1 x^{n-2} + \dots + a_{n-1} x + a_n = 0 \qquad (24)$$

met behulp van eene andere vergelijking

$$x^{n-1} = b_1 x^{n-2} + b_2 x^{n-3} + \dots + b_{n-2} x + b_{n-1} + y \qquad (25)$$

waarin de grootheden $b_1, \dots b_{n-1}$ voorloopig onbepaald bleven door eliminatie van x eene vergelijking

[1]) Cantor. Kapitel 66. [2]) Cantor. Kapitel 68.
[3]) Cantor. Kapitel 87.

$$y^n + c_1 y^{n-1} + \dots + c_{n-1} y + c_n = 0 \qquad (26)$$

af te leiden, waarin door eene geschikte keuze van de waarden $b_1, \dots b_{n-1}$ de grootheden $c_1, \dots c_{n-1}$ nul konden worden, zoodat de laatste vergelijking zou worden

$$y^n + c_n = 0.$$

Dit gaat goed, zoolang n 3 of 4 is. Voor $n = 5$ voert TSCHIRNHAUS echter de berekening niet door: trouwens hij moest stuiten op onoverkomelijke moeilijkheden.

§ 10. EULER (1707—1783) geeft in de „Comm. Acad. Petropol." van 1732 en 1733 eene verhandeling [1]), waarin hij de oplossing van vergelijkingen van den 2den, 3den 4den graad terugbrengt tot die van den 1sten, 2den, 3den graad.

Om de vergelijking

$$x^3 = ax + b \qquad (27)$$

op te lossen stelt hij b.v.

$$x = \sqrt[3]{A} + \sqrt[3]{B}. \qquad (28)$$

Hij vindt dan dat A en B de wortels zijn van de kwadratische resolvente (aequatio resolvens)

$$z^2 = bz - \frac{1}{27} a^3. \qquad (29)$$

Behalve $x_1 = \sqrt[3]{A} + \sqrt[3]{B}$ geeft hij nog de wortels

$$x_2 = \mu \sqrt[3]{A} + \nu \sqrt[3]{B} \quad \text{en} \quad x_3 = \nu \sqrt[3]{A} + \mu \sqrt[3]{B}$$

als μ en ν de complexe derdemachtswortels der eenheid zijn.

Voor de oplossing der vergelijking

$$x^4 = ax^2 + bx + c \qquad (30)$$

vindt hij op dergelijke wijze

$$x = \sqrt{A} + \sqrt{B} + \sqrt{C} \qquad (31)$$

---

[1]) CANTOR. Kapitel 105.

als A, B, C de wortels zijn der kubische resolvente.

$$z^3 = \frac{1}{2} a z^2 - \frac{1}{16}(4c + a^2) z + \frac{1}{64} b^2. \qquad (32)$$

De vier wortels zijn dan

$$x_1 = \sqrt{A} + \sqrt{B} + \sqrt{C} \qquad x_3 = -\sqrt{A} + \sqrt{B} - \sqrt{C}$$
$$x_2 = \sqrt{A} - \sqrt{B} - \sqrt{C} \qquad x_4 = -\sqrt{A} - \sqrt{B} + \sqrt{C}$$

Ook blijkt de vierdemachtsvergelijking oplosbaar te zijn met behulp van eene kubische resolvente, wanneer

$$x = \sqrt[4]{E} + \sqrt[4]{F} + \sqrt[4]{G}$$

wordt gesteld

Dit doet EULER vermoeden, dat bij elke vergelijking

$$x^n = a x^{n-2} + b x^{n-3} + \dots.$$

eene resolvente

$$z^{n-1} = \alpha z^{n-2} - \beta z^{n-3} + \gamma z^{n-4} - \dots.$$

te vinden moet zijn door

$$x = \sqrt[n]{A} + \sqrt[n]{B} + \sqrt[n]{C} + \dots.$$

te stellen. EULER meent ten onrechte, dat al geeft het vraagstuk hem voor $n = 5$ moeilijkheden, die moeilijkheden te overkomen zullen zijn en het vraagstuk ook in dit geval zal kunnen opgelost worden.

§ 11. BEZOUT [1]) lost de de derdemachtsvergelijking

$$x^3 + p x^2 + q x + r = 0$$

op door a en b in $y = \frac{x + a}{x + b}$ zóo te bepalen, dat door substitutie van deze waarde de vergelijking eene binomische wordt:

$$y^n + h = 0.$$

Het blijkt, dat a en b uit eene vierkantsvergelijking

[1]) Mémoires de l'Académie Royale des Sciences de Paris 1762, bldz. 17—52.

te bepalen zijn. y is dan uit de binomische vergelijking te vinden en daarna x uit $x = \frac{a - b y}{y - 1}$. De uitdrukking voor x wordt als men $p = 0$ stelt:

$$x = \sqrt[3]{a^2 b} + \sqrt[3]{a b^2}.$$

BEZOUT heeft getracht deze oplossingsmethode uit te breiden tot vergelijkingen van hoogeren graad. In

$$x^n + p x^{n-2} + q x^{n-3} + \ldots = 0$$

stelt hij weer $y = \frac{x + a}{x + b}$. Hij vindt dan natuurlijk, dat de coefficienten dezer vergelijking aan zekere voorwaarden moeten voldoen, wil de vergelijking in y, die door substitutie ontstaat, binomisch worden. Maar als aan de voorwaarden voldaan is, is de vergelijking oplosbaar en wordt

$$x = \sqrt[n]{a^{n-1} b} + \sqrt[n]{a^{n-2} b^2} + \ldots \sqrt[n]{a b^{n-1}}.$$

Het blijkt dus, dat BEZOUT zoo wel komt tot de oplossing van hoogere-machtsvergelijkingen van bepaalden vorm, maar niet tot die van algemeene vergelijkingen.

§ 12. Al deze pogingen hebben het vraagstuk van de algebraïsche oplossing van algemeene hoogere-machtsvergelijkingen twee eeuwen lang niet verder gebracht: men was in 't bezit van enkele oplossingsmethoden voor algemeene vergelijkingen van den derden en van den vierden graad, die zich niet lieten uitbreiden op vergelijkingen van hoogeren graad: men kon enkele hoogere-machtsvergelijkingen van bizonderen vorm oplossen, maar daarbij bleef het.

Eerst toen men tot combinatorische beschouwingen kwam, werden nieuwe gezichtspunten geopend. Deze waren reeds bij HUDDE, SAUNDERSON, LE SEUR te vinden [1]);

---

[1]) Vergelijk H. BURKHARDT. Die Anfänge der Gruppentheorie und PAOLO RUFFINI, in: Supplementband zu Zeitschr. für Math. u. Physik, 37ter Jahrgang 1892, Seite 120—159.

Waring (Miscellanea analytica, 1762) bewijst zelfs, dat de functiën van de wortels x_1, x_2, x_3, x_4 eener vierdemachtsvergelijking

$$x_1 x_2 + x_3 x_4, \quad (x_1 + x_2 - x_3 - x_4)^2, \quad (x_1 x_2 - x_3 x_4)^2$$

daar zij door permuteering der indices elk slechts drie verschillende vormen kunnen aannemen, uit kubische resolventen te vinden zijn, welker coefficienten in de coefficienten der vierdemachtsvergelijking kunnen uitgedrukt worden. Maar eerst de verschijning van twee belangrijke verhandelingen van Vandermonde en van Lagrange in 1770 brengt de oplossing van het vraagstuk verder.

§ 13. Vandermonde [1]) merkt op, dat een wortel a van de vierkantsvergelijking

$$x^2 - (a + b)x + ab = 0 \qquad (33)$$

eene functie van de coefficienten $a + b$ en ab moet zijn. Daar de vergelijking niet verandert, als men de wortels a en b verwisselt, moet b *dezelfde* functie van $a + b$ en ab zijn. Dit is alleen mogelijk, als de bedoelde functie tegelijk twee verschillende waarden kan voorstellen b.v.

$$\frac{1}{2}\left\{a + b + \sqrt{(a + b)^2 - 4ab}\right\} \qquad (34)$$

welke vorm in a overgaat als men voor den wortelvorm $a - b$ en in b, als men voor den wortelvorm $b - a$ schrijft.

Evenzoo behandelt Vandermonde de derdemachtsvergelijking

$$x^3 - (a + b + c)x^2 + (ab + bc + ca)x - abc = 0. \qquad (35)$$

Hij zoekt eene functie van $a + b + c$, $ab + bc + ca$ en abc, die naar verkiezing a, b of c kan worden. Het blijkt dat de uitdrukking

---

[1]) Mémoires de l'Académie des Sciences, année 1771. Paris 1774, p. 365—416.

$$\frac{1}{3}\left\{a+b+c+\sqrt[3]{(a+r'b+r''c)^3}+\sqrt[3]{(a+r''b+r'c)^3}\right\} \quad (36)$$

waarin r' en r'' complexe derdemachtswortels der eenheid zijn, gelijk aan a, b of c wordt, als men voor de daarin voorkomende wortelgrootheden neemt

$$\begin{array}{ccc} a+r'b+r''c & \text{en} & a+r''b+r'c\,, \\ r'(a+r'b+r''c) & \text{en} & r''(a+r''b+r'c) \quad \text{of} \\ r''(a+r'b+r''c) & \text{en} & r'(a+r''b+r'c). \end{array}$$

Het is nu de vraag of deze vorm te schrijven is als eene functie van $a+b+c$, $ab+bc+ca$ en abc alleen. Daarvoor zal 't in de eerste plaats noodig zijn dezen vorm zulk eene gedaante te geven, dat hij niet verandert, als men a, b en c onderling verwisselt. Het blijkt bij ontwikkeling der 3de machten onder de wortelteekens, dat deze door letterverwisseling slechts twee verschillende waarden kunnen aannemen:

$$(a+r'b+r''c)^3 = a^3+b^3+c^3 -$$
$$-\frac{3}{2}(a^2b+b^2c+c^2a+a^2c+b^2a+c^2b)+6abc+$$
$$+\frac{3}{2}(a^2b+b^2c+c^2a-a^2c-b^2a-c^2b)\sqrt{-3}.$$

De eenige verandering, die hierin door letterverwisseling kan ontstaan, is deze dat de vorm

$$a^2b+b^2c+c^2a-a^2c-b^2a-c^2b \quad (37)$$

van teeken verandert. VANDERMONDE vervangt deze door den wortel uit zijn kwadraat en zoo heeft (36) eene gedaante gekregen, die uiterlijk onveranderd blijft bij elke letterverwisseling. De vorm (36) is nu symmetrisch geschreven in a, b, c: het gelukt VANDERMONDE nu ook gemakkelijk, die waarde uit te drukken in de elementaire symmetrische functiën $a+b+c$, $ab+bc+ca$, abc.

Algemeen formuleert nu VANDERMONDE het vraagstuk aldus (p. 370):

On voit dès à présent que pour un degré quelconque la condition essentielle de la résolution générale étant de trouver une fonction de la somme des racines, de la somme de leurs produits deux à deux, de la somme de leurs produits trois à trois, etc., qui soit indifféremment l'une quelconque de ces racines, cette recherche peut se partager en trois chefs:

1°. trouver une fonction des racines de laquelle on puisse dire dans un certain sens qu'elle égale telle de ces racines que l'on voudra;

2°. mettre cette fonction sous une forme telle qu'il soit de plus indifférent d'y échanger les racines entre elles;

3°. y substituer les valeurs en somme de ces racines, somme de leurs produits deux à deux, etc.

VANDERMONDE neemt om 't 1ste deel van het vraagstuk op te lossen voor de n^{de} machtsvergelijking, de functie ($r', r'', \ldots$ zijn de wortels van $(r^n - 1):(r-1) = 0$):

$$\frac{1}{n}\Big[a + b + c + \ldots + \sqrt[n]{(a + r'b + r''c + \ldots)^n} + \\ + \sqrt[n]{(a + r'^2 b + r''^2 c + \ldots)^n} + \ldots + \\ + \sqrt[n]{(a + r'^{n-1} b + r''^{n-1} c + \ldots)^n}\Big]. \quad (38)$$

Neemt men voor de wortelgrootheden verschillende waarden, dan kan deze vorm inderdaad gelijk aan a, b, c, ... worden.

Ook met het 3de deel van 't vraagstuk stuit hij op geen enkel bezwaar: is eenmaal een vorm gevonden, die door geen enkele permutatie der a, b, c, ... verandert, dan kan deze symmetrische functie van de wortels altijd door de coefficienten der vergelijking worden uitgedrukt; zijne herleiding is echter, ook tengevolge van eene omslachtige en weinig doorzichtige notatie lang niet zoo eenvoudig als die door WARING ter zelfder tijd gegeven (vergelijk: SERRET. Algèbre supérieure, tome I, p. 385).

Bij het 2de deel van 't vraagstuk stuit VANDERMONDE

op moeilijkheden: bij de 3de- en de 4de-machtsvergelijkingen gaat alles goed, maar wanneer bij de 5de-machtsvergelijking de vorm (38) zóó geschreven zal worden, dat hij door letterverwisseling geen verandering ondergaat, blijkt dat niet zoo gemakkelijk te gaan; bij de 3de-machtsvergelijking bleek het eenige niet-symmetrische deel n.l. de zesterm (37) slechts twee verschillende waarden te kunnen aannemen, die zesterm was dus wortel van eene vierkantsvergelijking en wel, daar die twee waarden slechts in teeken verschilden, van eene zuivere vierkantsvergelijking. Bij de 5de-machtsvergelijking echter kwam VANDERMONDE op dezelfde wijze reeds tot eene resolvente van den 6den graad. Evenzoo bleek de oplossing eener zesdemachtsvergelijking af te hangen van die eener resolvente van den 10den of den 15den graad, die tot eene zesdegraadsresolvente terug te brengen was.

Resumeerende blijkt VANDERMONDE zich eene goede voorstelling gemaakt te hebben van den weg, dien men te gaan had om verder te komen: de meerwaardigheid van de functiën der wortels, het verband tusschen de functiën, die bij dezelfde permutaties der wortels onveranderd blijven, heeft hij in bizondere gevallen nagegaan; den graad van de vergelijking, waaruit zulk eene meerwaardige functie te vinden, zou zijn, wist hij aan te geven; op den *aard* der resolventen heeft hij nog niet gelet en daaraan is het te wijten, dat hij de onmogelijkheid der oplossing niet vermoed heeft. Daarvoor had hij trouwens moeten letten op het verband tusschen die permutaties der wortels, waarvoor zulk eene functie weer dezelfde waarde verkrijgt: hij had m.a.w. eene theorie der substituties moeten opbouwen. [1])

---

[1]) Eene Duitsche vertaling van de verhandeling van VANDERMONDE vindt men in: „Abhandlungen aus der reinen Mathematik von N. VANDERMONDE. In deutscher Sprache herausgegeben von CARL ITŽIGSOHN. Berlin JULIUS SPRINGER 1888".

§ 14. LAGRANGE is in dezelfde richting, hoewel in mindere mate te kort geschoten. Wat VANDERMONDE in bizondere gevallen inzag, het verband tusschen sommige functiën van de wortels, heeft LAGRANGE algemeen bewezen. Terecht geeft dus de geschiedschrijver van de Académie in 't jaarlijksch overzicht [1]) aan LAGRANGE den lof, dat hij bij zijn onderzoek meer het oog heeft gericht op de mogelijkheid der oplossing.

On verra qu'il [VANDERMONDE] s'est rencontré dans plusieurs points avec M. DE LA GRANGE, mais il paroît s'être plus particulièrement appliqué à simplifier les méthodes de calcul pour les rendre praticables tandis que M. DE LA GRANGE s'est plus occupé des moyens de s'assurer a priori de la possibilité de la solution cherchée ou de la généralité des méthodes connues."

LAGRANGE onderwerpt in zijne „Réflexions sur la théorie algébrique des équations" [2]) alle bekende methoden voor de oplossing van vergelijkingen aan een onderzoek. Hij begint met de oplossing van de derdemachtsvergelijking door HUDDE en merkt op, dat de wortelgrootheden, die in de uitdrukkingen voor de wortels

$$\left.\begin{aligned} a &= \sqrt[3]{-\frac{1}{2}p+\sqrt{q}}+\sqrt[3]{-\frac{1}{2}p-\sqrt{q}} \\ b &= \beta\sqrt[3]{-\frac{1}{2}p+\sqrt{q}}+\alpha\sqrt[3]{-\frac{1}{2}p-\sqrt{q}} \\ c &= \alpha\sqrt[3]{-\frac{1}{2}p+\sqrt{q}}+\beta\sqrt[3]{-\frac{1}{2}p-\sqrt{q}} \end{aligned}\right\} \quad (39)$$

voorkomen, waarin $q=\frac{1}{4}p^2+\frac{1}{27}n^3$ (vergelijk (20))

[1]) Histoire de l'Académie des Sciences, Année 1771 p. 49.

[2]) Nouveaux mémoires de l'Ac. R. des Sciences et belles-lettres de Berlin 1770 p. 134—135, 1771 p. 138—254.

en α en $\beta = \alpha^2$ de twee complexe derdemachtswortels uit de eenheid zijn, gemakkelijk rationaal in die wortels zijn uit te drukken. Men vindt

$$\left.\begin{aligned} \sqrt[3]{-\frac{1}{2}p + \sqrt{q}} &= \frac{1}{3}(a + \alpha b + \alpha^2 c) \\ \sqrt[3]{-\frac{1}{2}p - \sqrt{q}} &= \frac{1}{2}(a + \alpha^2 b + \alpha c) \end{aligned}\right\} \quad (40)$$

Deze functiën van de wortels worden bij de oplossing het eerst berekend: de wortels worden dan gevonden uit de 2 verschillende waarden, die de functie $a + \alpha b + \alpha^2 c$ bij verwisseling der wortels aanneemt.

Deze zelfde handelwijze past LAGRANGE nu toe op de volledige derdemachtsvergelijking

$$x^3 + mx^2 + nx + p = 0 \qquad (41)$$

Hij neemt [1]) de lineaire functie $Aa + Bb + Cc$ der wortels waarin A, B, C voorloopig willekeurige coëfficienten voorstellen. Deze functie zal uit een zesdemachtsvergelijking te vinden zijn, daar zij bij permuteering van de wortels 6 waarden kan krijgen:

$$\left.\begin{matrix} Aa + Bb + Cc & Ab + Ba + Cc & Ac + Ba + Cb \\ Aa + Bc + Cb & Ab + Bc + Ca & Ac + Bb + Ca \end{matrix}\right\} \quad (42)$$

Zal deze zesdemachtsvergelijking er eene worden van den tweedemachtsvorm, zoodat, als r een wortel is, ook αr en $\alpha^2 r$ wortels zullen zijn, dan zal men voor A, B, C moeten nemen 1, α, α^2; de 6 wortels worden dan

$$\left.\begin{matrix} r = a + \alpha b + \alpha^2 c, & \alpha r, & \alpha^2 r \\ s = a + \alpha c + \alpha^2 b, & \alpha s, & \alpha^2 s \end{matrix}\right\} \quad (43)$$

en de zesdemachtsvergelijking wordt

---

[1]) Art. 7 p. 144.

$$y^6 - (r^3 + s^3)\, y^3 + r^3s^3 = 0 \qquad (44)$$

$r^3 + s^3$ en r^3s^3 worden in de coefficienten der oorspronkelijke vergelijking uitgedrukt, y is dan te vinden en uit

$$a + \alpha b + \alpha^2 c = y_1,\ a + \alpha^2 b + \alpha c = y_2,\ a + b + c = -m \qquad (45)$$

zijn de wortels a, b, c te bepalen.

LAGRANGE onderwerpt aan een dergelijk onderzoek de methoden door TSCHIRNHAUS, EULER, BEZOUT gegeven; hij laat telkens zien, dat de schrijvers komen tot resolventen, waarvan de aard en de graad a priori zijn te te bepalen, als men slechts nagaat hoeveel verschillende waarden de optredende functien der wortels kunnen aannemen bij permutatie der wortels en hoe deze waarden samenhangen.

§ 15. LAGRANGE behandelt verder (Section II) de oplossingen der bikwadratische vergelijking. Naar aanleiding van de oplossing van VIETA (LAGRANGE noemt ze die van FERRARI) merkt hij op, dat de hulpgrootheden y en $\sqrt{2y - n}$, die het eerst bepaald worden (zie de vergelijkingen (7) — (10)) eenvoudige functiën van de wortels a, b, c en d zijn. Men vindt toch:

$$\left.\begin{aligned} y &= \frac{1}{2}(ab + cd) \\ \sqrt{2y - n} &= \frac{1}{2}(c + d - a - b) \end{aligned}\right\} \qquad (46)$$

Hierop grondt L. eene directe methode ter oplossing van de volledige vierdemachtsvergelijking:

$$x^4 + mx^3 + nx^2 + px + q = 0 \qquad (47)$$

Hij merkt op (art. 30), dat

$$u = ab + cd$$

eene functie der wortels is, die bij alle mogelijke permutaties der wortels slechts drie waarden kan aannemen:

$$\left.\begin{aligned} u_1 &= ab + cd \\ u_2 &= ac + bd \\ u_3 &= ad + bc \end{aligned}\right\} \qquad (48)$$

Deze functie moet dus te vinden zijn uit een vergelijking van den derden graad, welker coefficienten niet veranderen, als u_1, u_2, u_3 onderling verwisseld worden, dus ook niet bij permutatie van a, b, c, d. Deze coefficienten zijn dus symmetrische functiën van a, b, c, d en dus gemakkelijk in m, n, p, q uit te drukken.

Heeft men eene waarde van u, dan kan men, daar $abcd = q$ is, $v_1 = ab$ en $v_2 = cd$ vinden als wortels der vergelijking:

$$v^2 - u \, . \, v + q = 0 \qquad (49)$$

Verder is:

$$\left.\begin{aligned} -p &= ab\,(c + d) + cd\,(a + b) \\ -m &= \quad c + d \quad + \quad a + b \end{aligned}\right\} \qquad (50)$$

Derhalve kunnen $a + b$ en $c + d$ berekend worden en daarmee a, b, c en d afzonderlijk.

Men zou even goed, zegt LAGRANGE, van de functie der wortels

$$s = c + d - a - b \qquad (51)$$

gebruik kunnen maken. A priori is te zeggen, dat deze s uit eene zesdemachtsvergelijking met bekende coefficienten te vinden is, waarin (de 6 waarden van s zijn twee aan twee op het teeken na gelijk) niet anders dan even machten van s kunnen voorkomen en die dus als eene derdemachtsvergelijking is op te lossen.

Kent men éene waarde van s, dan is ook bekend:

$$ab + cd = \frac{s^2 - m^2 + 4\,n}{4}. \qquad (52)$$

en dan komt men gemakkelijk verder.

Op dezelfde wijze gaat LAGRANGE bij de andere oplossingen der 4de-machtsvergelijking na, welke rationale functie der wortels telkens bepaald wordt en hoe de

vorm der resolvente moet afhangen van de verschillende waarden, die deze functie bij onderlinge verwisseling van de wortels aanneemt.

§ 16 LAGRANGE gaat in de Mémoires van 't volgend jaar [1]) voort met de hoogere machtsvergelijkingen. Als te bepalen functie van de wortels $x', x'', x''' \ldots x^{(\mu)}$ neemt hij aan

$$x' + yx'' + y^2 x''' + \ldots\ldots y^{\mu-1} x^{(\mu)} \qquad (53)$$

waarin y eene primitieve μ^{de}-machtswortel der eenheid voorstelt. Het blijkt, dat voor deze functie eene oplosbare resolvente gevonden wordt in het geval van de derde- en vierdemachtsvergelijkingen, maar niet voor hoogere machten.

§ 17. Ten slotte en dit is wel het belangrijkste van deze verhandelingen, beschouwt LAGRANGE in onderling verband de rationale functiën der wortels, die bij dezelfde permutaties dier wortels onveranderd blijven (fonctions semblables). Hij laat zien, dat alle „gelijksoortige" functiën aan resolventen van *denzelfden* graad voldoen en dat die graad altijd zal zijn $1.2.3.\ldots.\mu$ of een deeler daarvan; hij spoort het verband op tusschen rationale functiën die niet voor dezelfde permutaties der wortels onveranderd blijven. Hij vindt zoo [2]) zijne bekende stelling: zijn de substituties, die eene functie t onveranderd laten begrepen onder die, welke de functie y niet veranderen, dan kan y rationaal worden uitgedrukt in t en de coefficienten der vergelijking. Zijn echter de substituties, die y onveranderd laten, begrepen onder die welke t niet veranderen en is er onder elke m substistuties, die t onveranderd laten telkens ééne, die y onveranderd laat, dan wordt y gevonden als wortel van eene m^{de}-machtsvergelijking, welker coefficienten rationaal in

[1]) 1771, p. 138—254
[2]) Art. 100—104.

t en in de coefficienten der vergelijking zijn uit te drukken.

§ 18. Lichten we deze stellingen even toe aan de voorbeelden, die boven behandeld zijn.

a). Derdemachtsvergelijking (41). Alle mogelijke permutaties der wortels kunnen de volgorde a, b, c der wortels veranderen in

1. $a\,b\,c$	3. $b\,c\,a$	5. $c\,a\,b$
2. $a\,c\,b$	4. $b\,a\,c$	6. $c\,b\,a$ [1]).

De functie $(a + \alpha b + \alpha^2 c)^3$ blijft onveranderd door de permutaties 1, 3, 5, d. i. door telkens éene van 2 permutaties, die symmetrische functiën der wortels onveranderd laten. Deze functie is dus te vinden uit eene vierkantsvergelijking met bekende coefficienten [verg.(44)].

De functie $a + \alpha b + \alpha^2 c$ blijft alleen onveranderd door de permutatie 1 der wortels, d. i. door éene van de drie, die $(a + \alpha b + \alpha^2 c)^3$ onveranderd laten. $a + \alpha b + \alpha^2 c$ is dus uit eene derdemachtsvergelijking te vinden, als $(a + \alpha b + \alpha^2 c)^3$ bekend is.

b). Vierdemachtsvergelijkingen (47). Alle mogelijke permutaties der wortels kunnen de volgorde $abcd$ veranderen in

1. $a\,b\,c\,d$	7. $b\,a\,c\,d$	13. $c\,a\,b\,d$	19. $d\,a\,b\,c$
2. $a\,b\,d\,c$	8. $b\,a\,d\,c$	14. $c\,a\,d\,b$	20. $d\,a\,c\,b$
3. $a\,c\,d\,b$	9. $b\,c\,d\,a$	15. $c\,b\,d\,a$	21. $d\,b\,c\,a$
4. $a\,c\,b\,d$	10. $b\,c\,a\,d$	16. $c\,b\,a\,d$	22. $d\,b\,a\,c$
5. $a\,d\,b\,c$	11. $b\,d\,a\,c$	17. $c\,d\,a\,b$	23. $d\,c\,a\,b$
6. $a\,d\,c\,b$	12. $b\,d\,c\,a$	18. $c\,d\,b\,a$	24. $d\,c\,b\,a$.

De functie $u = ab + cd$ verandert niet door de acht

[1]) Om licht begrijpelijke redenen moet de permutatie, die de volgorde $a\,b\,c$ verandert in de volgorde $a\,b\,c$, die dus eigenlijk niets verandert, toch meegeteld worden.

permutaties 1, 2, 7, 8, 17, 18, 23, 24 d. i. door telkens ééne van elke drie permutaties, die de symmetrische functiën der wortels onveranderd laten. De functie u wordt dus uit eene derdemachtsvergelijking gevonden.

De functie $v = ab$ blijft alleen onveranderd door de permutaties 1, 2, 7, 8, die onder dit achttal voorkomen en, daar van elke *twee* permutaties van het achttal er eene bij dit viertal is, wordt v gevonden uit eene vergelijking van den tweeden graad, welker coefficienten rationaal in u en de coefficienten der vergelijking zijn uit te drukken.

De functie $s = c + d - a - b$ (51) blijft alleen onveranderd door de permutaties 1, 2, 7, 8, d. i. door ééne permutatie op elke zes, die de symmetrische functiën van a, b, c, d onveranderd laten. s kan dus uit eene zesdemachtsvergelijking gevonden worden. s^2 blijft bovendien onveranderd door de permutaties 17, 18, 23, 24, dus door ééne op elke drie permutaties, die symmetrische functiën onveranderd laten. Daarom zal men weer eerst s^2 uit eene derdemachtsvergelijking en daarna s uit eene vierkantsvergelijking berekenen.

Lagrange zegt ten slotte [1]: „Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme l'on voit, à une espece de calcul des combinaisons par lequel on trouve a priori les résultats auxquels on doit s'attendre Il seroit à propos d'en faire l'application aux équations du cinquième degré et des degrés supérieurs dont la résolution est jusqu'à présent inconnue; mais cette application demande un trop grand nombre de recherches et de combinaisons, dont le succès est d'ailleurs fort douteux, pourque nous puissions quant à présent nous livrer à ce travail."

Lagrange heeft zich ook later niet aan dit werk begeven,

[1]) Art. 109.

maar hun, die na hem kwamen, heeft hij in de besproken verhandeling duidelijk aangewezen in welke richting zij verder te werken hadden. Functiën van de wortels moesten in de coefficienten der vergelijking worden uitgedrukt, andere functiën met een grooter aantal verschillende waarden in deze functiën en zoo moest men voortgaan totdat men de wortels zelve had. Het kwam er dus op aan functiën der wortels op hare veelwaardigheid te onderzoeken, de permutaties der wortels, waardoor deze functiën onveranderd bleven, te vergelijken met die, waarvoor andere functiën niet veranderden. De permutaties, die eene functie onveranderd laten, moeten in de geheele verzameling der $n!$ permutaties een afgesloten geheel vormen, daar de achtereenvolgende toepassing van deze permutaties en de herhaalde toepassing van eene dezer permutaties natuurlijk gelijkwaardig moeten zijn met eene enkele permutatie van het stel. Het kwam dus ten slotte daarop aan, dat men naging op welke wijzen men uit de $n!$ permutaties zulke verzamelingen kon afscheiden en welk het verband moest zijn tusschen deze verzamelingen onderling en deze verzamelingen vergeleken met het totaal van alle permutaties, opdat de resolventen, waartoe men kwam, algebraisch oplosbaar werden.

§ 19. Het is Paolo Ruffini geweest, die in zijn leerboek Teoria generale delle Equazioni (Bologna, 1799) het eerst het vraagstuk op deze wijze heeft aangevat. Ruffini behandelt vooraf in een afzonderlijk hoofdstuk wat hij noemt permutaties, dat zijn verzamelingen van permutaties zooals wij zooeven aantroffen, die een in zich zelf gesloten geheel vormen en nu substitutiegroepen genoemd worden. Hij bestudeert deze groepen voor 't eerst losgemaakt van de theorie der hoogere-machtsvergelijkingen en hij past daarop later zijne resultaten toe. Bij de behandeling der substitutiegroepen zullen we hier en daar gelegenheid vinden aan te teekenen wat men reeds aan Ruffini verschuldigd is. Merken we nu alleen op, dat Ruffini al

tot allerlei algemeene eigenschappen komt; dat hij na deze algemeene beschouwingen de groepen van vijf elementen en de veelwaardigheid van functiën dier elementen aan een gedetailleerd onderzoek onderwerpt en dat hij zoo o. a. tot het besluit komt, dat er geen drie-, vier- en achtwaardige functiën van vijf elementen kunnen bestaan. Voor het eerst komt RUFFINI zoo tot de algebraïsche onoplosbaarheid van de algemeene vijfdemachtsvergelijking. Nu zijn tegen dit bewijs verschillende bedenkingen aan te voeren, die men uitvoerig behandeld vindt in de boven geciteerde verhandeling van BURKHARDT; bedenkingen, waarvan de voornaamste niet is weggenomen door de latere verhandelingen van den schrijver; het is n. l. de vraag of men het recht heeft zich in al deze beschouwingen te bepalen tot *rationale* functiën van de wortels en of het niet mogelijk zou zijn tot eene oplossing te komen door als hulpgrootheden te nemen functiën, die niet rationaal zijn in de wortels der vergelijking.

§ 20. ABEL [1]), die onbekend was met het bewijs van RUFFINI, heeft in zijn bewijs deze fout ontgaan door met behulp van onnoodig gecompliceerde berekeningen aan te toonen, dat, als eene vergelijking door worteltrekkingen oplosbaar is, de wortelgrootheden, die in de oplossing voorkomen, altijd geheele rationale functiën zijn van de wortels der vergelijking en van wortels der eenheid, waarbij de coefficienten dezer functiën rationale getallen zijn. KRONECKER [2]) heeft ABEL's bewijs, vooral wat de berekeningen betreft, vereenvoudigd en nog onlangs is dit bewijs door PIERPONT [3]) niet alleen wat de algebraische berekeningen maar ook wat de theorie der substituties betreft, tot zoo groot mogelijke vereenvoudiging gebracht.

§ 21. Zijn de beschouwingen van RUFFINI voor het

---

[1]) CRELLE's Journal Bnd I, 1826; Oeuvres Complètes, ed. Holmboe 1839, bldz. 5; ed. SYLOW et LIE 1881, bldz. 66.

[2]) Berliner Monatsberichte van Maart 1879 (bldz. 205).

[3]) Bull. Amer. Mathem. Society, April 1896 (bldz. 200—221).

vraagstuk der oplosbaarheid van hoogere-machtsvergelijkingen niet afdoende geweest, zij hebben in elk geval voor dit vraagstuk de verdienste, dat zij voor 't eerst op goede gronden aan de oplosbaarheid hebben doen twijfelen. Voor de theorie der substitutiegroepen zijn zij zeker van fundamenteel belang geweest. Want zij vullen voor een groot deel de bekende verhandeling van CAUCHY [1]), die als eerste proeve van eene theorie der substitutiegroepen te beschouwen is. Dat deze uitkomsten dikwijls aan CAUCHY toegeschreven worden, vindt zeker zijn grond hierin, dat CAUCHY RUFFINI niet dan terloops noemt. [2]) CAUCHY is echter niet bij de resultaten van RUFFINI blijven staan: hij heeft ze niet alleen systematisch en doorzichtig gerangschikt en door geschikte notaties aantrekkelijker gemaaakt, hij heeft ook menige stelling uitgebreid en menige nieuwe eigenschap gevonden CAUCHY heeft op het gebied der substitutiegroepen het materiaal bijeengebracht, dat GALOIS vervolgens voor het vraagstuk van de oplosbaarheid der hoogere-machtsvergelijkingen gebruikt heeft.

---

[1]) Journ. de l'Éc Pol., 17me Cahier t. X. 1815, bldz. 1: Sur le nombre des valeurs, qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme. Later uitvoeriger in: Exercices d'analyse et de physique mathématique t. III, 1846, bldz. 151.

[2]) Eenmaal noemt hij RUFFINI op bldz. 1, waar hij zegt „depuis ce temps [LAGRANGE, VAN DER MONDE 1771] quelques géomètres italiens se sont occupés avec succès de cette matière et particuliérement M. RUFFINI, qui a consigné le résultat de ses recherches dans le tome XII des Mem. de la soc. ital. et dans sa Théorie des équations numériques." Eenige bladzijden verder vindt men [bldz. 8]: „si n est égal à 5 ou surpasse 5 on n' [en] pourra plus former de semblables [fonctions qui aient seulement trois valeurs différentes]; on ne peut pas même dans ce cas former des fonctions qui n'aient que quatre valeurs. Ces deux propositions ont été démontrées par M. PAOLO RUFFINI dans les mémoires de la soc. ital. t. XII et dans sa Théorie des équations." Bij deze citaten blijft het.

§ 22. GALOIS [1]) heeft de vraag naar de oplosbaarheid van eene vergelijking door worteltrekking teruggebracht tot een vraagstuk van de theorie der substitutiegroepen. De eigenschapppen van elke hoogere-machtsvergelijking vindt hij afgebeeld in die eener door hem gedefinieerde groep van substituties tusschen de wortels der vergelijking n.l. die substituties, die elke rationale functie der wortels numeriek onveranderd laten. Opdat eene vergelijking door worteltrekkingen oplosbaar zij, moet de groep der vergelijking op eene zeer bijzondere wijze zijn samengesteld. De resolventen, waarom het reeds volgens LAGRANGE te doen is, moeten voor de oplosbaarheid door wortelgrootheden, binomiaalvergelijkingen zijn. GALOIS heeft nu nagegaan hoe de groep der vergelijking moet zijn, opdat de achtereenvolgende resolventen binomiaalvergelijkingen worden. Het is hem gebleken, dat in dit geval binnen de groep der vergelijking achtereenvolgens nieuwe groepen van substituties moeten gevon-

---

[1]) GALOIS had zijne denkbeelden neergelegd in eene verhandeling, die hij in 1831 aan de Fransche Académie des Sciences aanbood; de rapporteurs, LA CROIX en POISSON, vonden het stuk onbegrijpelijk; het werd niet opgenomen en is verloren gegaan

Het volgend jaar kwam GALOIS in een duel om (voor biografische bizonderheden moge verwezen worden naar: P. DUPUY. La vie d'ÉVARISTE GALOIS in Ann. Scientif. de l'Ecole Normale supérieure, série 3, t. XIII bldz. 197—266). Zijne uitkomsten over de voorwaarden der oplosbaarheid van vergelijkingen door wortelgrootheden, die hij gedeeltelijk op den avond vóor zijn dood opgeschreven heeft, zijn eerst in 1846 door zijn vriend CHEVALIER, dien hij met de publiceering belast had, aan LIOUVILLE ter hand gesteld; zij hebben met zijne andere werken eene plaats gevonden in tome XIII van LIOUVILLE's Journal. De Société mathém. de France heeft in 1897 zijne werken opnieuw uitgegeven (Oeuvres mathématiques d'Év. GALOIS. Paris, GAUTHIER—VILLARS et Fils). Eene Duitsche vertaling van de werken van GALOIS en die van ABEL over de vergelijkingen is door MASER bezorgd; de titel is: Abhandlungen über die algebraische Auflösung der Gleichungen von N. H. ABEL und E. GALOIS. Berlin, SPRINGER 1889.

den kunnen worden, die in elke voorafgaande groep eene zeer bizondere plaats innemen. In deze inleiding kunnen we hierop niet verder ingaan: het zij voldoende, op te merken, dat de groepen van substituties, die bij de algemeene hoogeremachtsvergelijkingen behooren, deze bijzonderheden in de samenstelling niet vertoonen zoodra de graad der vergelijking > 4 is. Daarmee heeft GALOIS de onmogelijkheid van de algebraïsche oplossing van vergelijkingen van hoogeren dan den vierden graad aangewezen; wat meer is, hij heeft een kriterium voor de algebraïsche oplosbaarheid van hoogeremachtsvergelijkingen gegeven en zoo de mogelijkheid geopend, om voor elke bijzondere vergelijking uit te maken of zij al dan niet door wortelgrootheden oplosbaar is.

GALOIS' verhandelingen zijn door hare groote beknoptheid, begrijpelijk door de omstandigheden waaronder zij zijn ontstaan, bijna onverstaanbaar voor hem, die zich niet eerst langs anderen weg in de theorie van GALOIS heeft ingewerkt; de schrijver heeft er den avond vóor zijn dood in de grootste haast nog allerlei wijzigingen in aangebracht, geen wonder dus, dat er later heel wat commentaren op zijn verschenen.

Voor het eerst zijn GALOIS' stellingen streng bewezen door BETTI [1]). SERRET heeft ze opgenomen in den tweeden druk van zijn Algèbre supérieure (1854), JORDAN eindelijk heeft ze gecommentarieerd in de Comptes Rendus, tome LX en in de Mathematische Analen, Band I en wat op dat oogenblik van substitutiegroepen bekend was, meegedeeld in zijn standaardwerk: Traité des substitutions et des équations algébriques Paris, GAUTHIER-VILLARS ET FILS, 1870. Daarna vindt men de theorie der substitutiegroepen nog behandeld in E. NETTO, Substitutionentheorie, Leipzig, TEUBNER 1882; VOGT, Leçons sur la résolution algébrique des équations, Paris, NONY

---

[1]) TORTOLINI Annali di Scienze fisiche e matematiche, t. IV, 1853.

& CIE., 1895 en in de standaardwerken: H. WEBER, Lehrbuch der Algebra I, II, Braunschweig, VIEWEG, 1895—96 [1]) en BURNSIDE, Theory of groups of finite order. Cambridge 1897.

We gaan nu eerst over tot eene korte behandeling der substitutiegroepen en komen daarna tot hare toepassing op de vraag naar de algebraïsche oplosbaarheid der hoogere-machtsvergelijkingen.

---

[1]) Van dit werk is reeds een 2de druk verschenen.

HOOFDSTUK II.

EENVOUDIGE EIGENSCHAPPEN DER SUBSTITUTIE-GROEPEN.

§ 23. De bewerking, waardoor m grootheden x_0, x_1, ... x_{m-1} resp. overgevoerd worden in de grootheden x_{i_0}, x_{i_1}, ... $x_{i_{m-1}}$ (i_0, i_1, ... i_{m-1} stellen de indices 0, 1, ... $m - 1$ in andere volgorde voor), heet eene substitutie. De substitutie doet dus de rangschikking $x_0 x_1 \ldots x_{m-1}$ overgaan in $x_{i_0} x_{i_1} \ldots x_{i_{m-1}}$.

§ 24. Past men op de rangschikking $x_0 x_1 \ldots x_{m-1}$ achtereenvolgens twee substituties toe, dan krijgt men eene rangschikking, die ook door ééne substitutie kan verkregen worden, die dan het product der eerste twee heet.

§ 25. Het product van twee substituties mist in het algemeen de commutatieve eigenschap. Immers, als men eene substitutie s, die x_i door x_j vervangt, laat volgen door eene substitutie t, die x_j in x_k overvoert, dan zal het product st de grootheid x_i in x_k overvoeren; maar in welke grootheid x_i door het product ts zal overgevoerd werden, is uit hetgeen van de substituties s en t gezegd is, nog volstrekt niet af te leiden. Js in een gegeven geval st dezelfde substitutie als ts, dan heeten s en t verwisselbaar of commutatief. Twee substituties zijn altijd verwisselbaar, als zij geen enkel gemeenschappelijk element bevatten.

§ 26. Onder het gedurig produkt $s\,t\,u\ldots.$ der substituties s, t, $u,\ldots.$ verstaat men de substitutie, die $x_0\ x_1,\ldots.\ x_{m-1}$ in die rangschikking overvoert, welke ontstaat, wanneer men eerst de substitutie s, daarna t, vervolgens $u,\ldots.$ uitvoert. De vermenigvuldiging bezit blijkbaar de associatieve eigenschap

$$(s\,t)\,u = s\,(t\,u)$$

want als s 't element x_i in x_j, t x_j in x_k en u x_k in x_l overvoert, dan voert zoowel $(s\,t)\,u$ als $s\,(t\,u)$ 't element x_i in x_l over.

§ 27. Eene substitutie kan op verschillende wijzen worden voorgesteld. Men kan b.v. onder de aanvankelijke (of eene andere) rangschikking der elementen x_0, $x_1,\ldots.\ x_{m-1}$ de rangschikking schrijven, waarin deze door de substitutie wordt overgevoerd, aldus:

$$\begin{pmatrix} x_0\, x_1\, x_2 \ldots\ldots\ldots x_{m-1} \\ x_{i_0}\, x_{i_1}\, x_{i_2} \ldots\ldots\ldots x_{i_{m-1}} \end{pmatrix}$$

Telt men de substitutie

$$\begin{pmatrix} x_0\, x_1\, x_2 \ldots\ldots\ldots x_{m-1} \\ x_0\, x_1\, x_2 \ldots\ldots\ldots x_{m-1} \end{pmatrix}$$

die de identische substitutie of de eenheid heet en dikwijls door 't symbool 1 wordt voorgesteld, mede, dan is het totale aantal substituties van m grootheden $m!$

§ 28. Eene andere schrijfwijze wordt dikwijls gebruikt: voert eene substitutie x_i in x_j, x_j in x_k, x_k in x_l, enz. en eindelijk x_p in x_i over, dan schrijft men deze

$$(x_i\ x_j\ x_k\ x_l \ldots.\ x_p) \quad \text{of} \quad (x_j\ x_k\ x_l \ldots.\ x_p\ x_i),\ \text{enz.}$$

Men zegt, dat deze verwisselingen een cyclus vormen en noemt deze substitutie eene cyclische of circulaire.

Elke substitutie kan als een product van cyclische geschreven worden, zoodat elk element maar in één cyclus voorkomt. De substitutie

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 \\ x_2 & x_7 & x_9 & x_0 & x_1 & x_8 & x_6 & x_4 & x_5 & x_3 \end{pmatrix}$$

kan b.v. geschreven worden

$(x_0\, x_2\, x_9\, x_3)\,(x_1\, x_7\, x_4)\,(x_5\, x_8)\,(x_6)$ of $(x_0\, x_2\, x_9\, x_3)\,(x_1\, x_7\, x_4)\,(x_5\, x_8)$

daar een cyclus van één element gewoonlijk wordt weggelaten. De volgorde der cycli is natuurlijk willekeurig.

§ 29. Eene substitutie, wier cycli op deze wijze evenveel elementen bevatten, heet eene regelmatige substitutie, b.v.

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 \\ x_4 & x_5 & x_3 & x_2 & x_0 & x_1 \end{pmatrix} = (x_0\, x_4)\,(x_1\, x_5)\,(x_2\, x_3).$$

§ 30. Een cyclus van 2 elementen heet eene transpositie.

Daar men uit elke permutatie tot elke andere permutatie kan komen door herhaaldelijk telkens slechts twee elementen te verwisselen, kan elke substitutie als een product van transposities geschreven worden; elk element behoeft echter nu niet in slechts één cyclus voor te komen. Deze ontbinding in transposities kan zelfs op verschillende wijzen plaats hebben. Eene zelfde substitutie zal echter in alle gevallen een even aantal transposities of in alle gevallen een oneven aantal transposities opleveren [1]).

§ 31. Beschouwen we om dit te bewijzen eene substitutie van n letters, die i cycli bevat; laat deze substitutie als een product van τ transposities geschreven kunnen worden. Laat men op deze τ transposities dezelfde τ transposities in omgekeerde rangorde volgen, dan krijgt men daar $(x_i\, x_j)\,(x_i\, x_j) = 1$, de identische substitutie, die m cycli bevat, elk van één element. Wat gebeurt er echter met het aantal cycli wanneer men deze τ transposities laat volgen op de i cycli en deze transposities zooveel mogelijk met de andere cycli samenstelt? Vermenigvuldigt men met eene

[1]) JORDAN, Traité des substitutions, blz. 61.

transpositie $(x_i\,x_j)$ dan komt er één cyclus bij of gaat er één cyclus af al naar gelang x_i en x_j in één cyclus of in 2 verschillende cycli voorkomen; want

$$(x_a\,..\,x_b\,x_i\,x_c\,..\,x_d\,x_j\,x_e\,..\,x_f)(x_i\,x_j) = (x_a\,..\,x_b\,x_j\,x_e\,..\,x_f)(x_i\,x_c\,..\,x_d)$$

en $(x_a\;.\,x_b\,x_i\,x_c\,..\,x_d)(x_{a'}\,..\,x_{b'}\,x_j\,x_{c'}\,..\,x_{d'})(x_i\,x_j) =$

$$= (x_a\,..\,x_b\,x_j\,x_{c'}\,..\,x_{d'}\,x_{a'}\,..\,x_{b'}\,x_i\,x_c\,..\,x_d)$$

Vermenigvuldigt men achtereenvolgens met τ transposities, dan komen er dus, op een tweevoud na, τ cycli bij; derhalve is $i+\tau$ op een tweevoud na gelijk aan m, dus 't aantal transposities $\tau = m - i$ op een tweevoud na. Is $m - i$ even, dan is 't aantal transposities even, anders oneven.

Men spreekt van eene even substitutie of eene oneven substitutie naar gelang zij als een product van een even aantal of van een oneven aantal transposities kan geschreven worden.

§ 32 Bij eene derde schrijfwijze voor eene substitutie let men op de waarden der indices, die elkaar vervangen.

Is de waarde van $\varphi\,(z)$ voor $z = 0, 1, 2, \ldots m-1$ gelijk aan $i_0, i_1, i_2, \ldots i_{m-1}$, dan kan men de substitutie

$$\begin{pmatrix} x_0\, x_1\, x_2 \ldots x_{m-1} \\ x_{i_0} x_{i_1} x_{i_2} \ldots x_{i_{m-1}} \end{pmatrix} \text{ schrijven } \begin{pmatrix} x_z \\ x_{\varphi(z)} \end{pmatrix}$$

of eenvoudig $[z\;\varphi(z)]$. [1])

Voor $\varphi(z)$ kan men met behulp van de interpolatieformule van LAGRANGE b. v. schrijven

$$\varphi\,(z) = \frac{i_0\,F\,(z)}{z.\,F'(0)} + \frac{i_1\,F\,(z)}{(z-1)F'(1)} + \ldots\ldots \frac{i_{m-1}\,F\,(z)}{(z-m+1)F'(m-1)}$$

als $F(z) \equiv z\,(z-1)\,(z-2)\,\ldots\ldots\,(z-m+1)$. Overigens heeft HERMITE (Comptes Rendus, t. 57) de voorwaarde gegeven, waaraan $\varphi\,(z)$ moet voldoen om in dit geval bruikbaar te wezen.

[1]) Deze notatie is van JORDAN (bldz. 88.).

Als men twee indices als gelijk beschouwt, die congruent zijn modulo m, kan men ook indices $> m - 1$ toelaten. De circulaire substitutie $(x_0 x_1 x_2 \ldots . x_{m-1})$ kan men dan b.v. voorstellen door $[z \;\; z+1]$ (mod. m).

§ 33. Door de herhaling van eene zelfde substitutie s ontstaat eene macht van die substitutie; men schrijft $s^2, s^3, \ldots .$ Is b.v. $s = (x_0 x_1 x_2 x_3 x_4 x_5)$, dan is

$s^2 = (x_0 x_2 x_4)(x_1 x_3 x_5)$, $s^3 = (x_0 x_3)(x_1 x_4)(x_2 x_5)$

$s^4 = (x_0 x_4 x_2)(x_1 x_5 x_3)$ $s^5 = (x_0 x_5 x_4 x_3 x_2 x_1)$

of in andere schrijfwijze:

$s = [z \;\; z+1], s^2 = [z \;\; z+2], s^3 = [z \;\; z+3], s^4 = [z \;\; z+4]$
$s^5 = [z \;\; z+5]$, alles modulo 6.

De machten eener zelfde substitutie zijn commutatief.

§ 34. De substitutie, die na eene andere s uitgevoerd, weer de oorspronkelijke rangschikking doet ontstaan, heet de *omgekeerde* of *inverse substitutie* van s; men stelt ze voor door s^{-1}. Is

$$s = \begin{pmatrix} x_0 x_1 \ldots . . x_{m-1} \\ x_{i_0} x_{i_1} \ldots . x_{i_{m-1}} \end{pmatrix} \text{ dan is } s^{-1} = \begin{pmatrix} x_{i_0} x_{i_1} \ldots . x_{i_{m-1}} \\ x_0 x_1 \ldots . . x_{m-1} \end{pmatrix}.$$

s is de omgekeerde van s^{-1}. De omgekeerde van $s_1 s_2$ is $s_2^{-1} s_1^{-1}$, want $s_1 s_2 . s_2^{-1} s_1^{-1} = 1$.

§ 35. Schrijft men de achtereenvolgende machten eener substitutie s van m letters $x_0, \ldots . x_{m-1}$ op, dan zullen niet voortdurend nieuwe substituties ontstaan, omdat het aantal substituties van m letters eindig is. Zij s^β de eerste substitutie in de reeks $s, s^2, s^3, \ldots \ldots$ die aan eene vorige s^α gelijk is. Dan is

$$s^{\beta-\alpha} s^\alpha = s^\alpha$$

en dus door vermenigvuldiging met de omgekeerde van s^α:

$$s^{\beta-\alpha} = 1.$$

Het getal $\beta - \alpha = \mu$, de exponent van de laagste macht van s, die gelijk aan de identische substitutie is,

heet de *orde* der substitutie. De orde eener cyclische substitutie is blijkbaar gelijk aan het aantal letters, die zij verplaatst; de orde eener willekeurige substitutie is het kleinst gemeene veelvoud van de orden der cycli waaruit zij bestaat.

§ 36. Is $s^\mu = 1$, dan is $s^{\mu+\alpha} = s^\alpha$. Ook is $s^{\mu-\alpha} s^\alpha = 1$, dus $s^{\mu-\alpha} = (s^\alpha)^{-1}$. Voor $s^{\mu-\alpha}$ schrijft men ook $s^{-\alpha}$. Voor s^μ ook $s^0 = 1$. Alle geheele positieve en negatieve machten eener substitutie zijn hiermee ingevoerd: twee machten zijn identiek, als hare exponenten congruent zijn mod. μ.

§ 37. Twee substituties heeten *gelijkvormig*, als zij alleen verschillen in de elementen, waarop zij opereeren: zij bezitten dus hetzelfde aantal cycli en het aantal elementen, in elken cyclus voorkomende, stemt in de eene substitutie overeen met dat in de andere substitutie. Zoo zijn

$$s = (x_0\, x_2\, x_3)\,(x_1\, x_4) \quad \text{en} \quad t = (x_1\, x_3\, x_4)\,(x_0\, x_2)$$

gelijkvormig. De eene kan gemakkelijk in de andere overgevoerd worden met behulp van eene andere substitutie en hare omgekeerde. Voert men n.l. eerst de elementen x_1, x_3, x_4, x_0, x_2 over resp. in x_0, x_2, x_3, x_1, x_4, past men daarna de substitutie s toe en brengt men daarna x_0, x_2, x_3, x_1, x_4 weer over in x_1, x_3, x_4, x_0, x_2, dan heeft men eene letterverplaatsing gekregen, die in eens door t bewerkt kan worden. Men zegt nu, dat t ontstaat, als s getransformeerd wordt door de substitutie

$$\sigma = \begin{pmatrix} x_0\, x_2\, x_3\, x_1\, x_4 \\ x_1\, x_3\, x_4\, x_0\, x_2 \end{pmatrix}.$$

Men heeft dan $t = \sigma^{-1} s\, \sigma$ en men vindt t door de de substitutie σ toe te passen op de elementen, zooals zij voorkomen in s, als deze in cycli geschreven is.

§ 38. Eene verzameling van substituties heet eene

groep [1]), als het product van elke twee ervan tot de verzameling behoort. Elke groep bevat blijkens het voorgaande de omgekeerde van elke substitutie en de identische substitutie.

Het aantal substituties eener groep heet hare *orde* [2]), het aantal letters, waarop de substituties worden toegepast, haar *graad.*

§ 39. Voorbeelden. 1. Alle $m!$ substituties van m letters vormen een groep, de *symmetrische groep* geheeten. Voor 4 letters schrijft men de substituties gemakkelijk op door de onderlinge permutaties der 4 letters te vergelijken met de oorspronkelijke rangschikking. Men vindt:

1. 1	5. $(x_1 x_3 x_2)$	9. $(x_0 x_1 x_2 x_3)$	13. $(x_0 x_2 x_1)$	17. $(x_0 x_2)(x_1 x_3)$	21. $(x_0 x_3)$
2. $(x_2 x_3)$	6. $(x_1 x_3)$	10. $(x_0 x_1 x_2)$	14. $(x_0 x_2 x_3 x_1)$	18. $(x_0 x_2 x_1 x_3)$	22. $(x_0 x_3 x_2)$
3. $(x_1 x_2 x_3)$	7. $(x_0 x_1)$	11. $(x_0 x_1 x_3 x_2)$	15. $(x_0 x_2 x_3)$	19. $(x_0 x_3 x_2 x_1)$	23. $(x_0 x_3 x_1 x_2)$
4. $(x_1 x_2)$	8. $(x_0 x_1)(x_2 x_3)$	12. $(x_0 x_1 x_3)$	16. $(x_0 x_2)$	20. $(x_0 x_3 x_1)$	24. $(x_0 x_3)(x_1 x_2)$

2. De substituties in de symmetrische groep, die als een product van een even aantal transposities kunnen geschreven worden, vormen samen ook eene groep, de *alterneerende groep* geheeten. Want het product van twee dezer substituties kan ook als een product van een even aantal transposities geschreven worden en behoort dus tot de verzameling. De alterneerende groep bevat alle cyclische substituties van drie elementen en elk harer substituties kan als een product van cycli van drie elementen geschreven worden, want:

$$(x_i x_j)(x_i x_k) = (x_i x_j x_k) \quad \text{en} \quad (x_i x_j)(x_k x_l) = (x_i x_k x_l)(x_i x_k x_j)$$

Bevat eene groep alle cyclische substituties van drie elementen, waarin de eerste twee twee vaste elementen zijn, n.l. $(x_0\, x_1\, x_2)$, $(x_0\, x_1\, x_3)$, $(x_0\, x_1\, x_4)$, enz. dan bevat zij

[1]) Het woord groep is afkomstig van GALOIS. Zie Oeuvres de GALOIS. Paris 1897. Bldz. 36.

[2]) Dit begrip is door RUFFINI ingevoerd.

de alterneerende groep. Elke cyclische substitutie toch van drie elementen kan, het blijkt uit het volgende, als een product van deze substituties $(x_0\, x_1\, x_i)$ geschreven worden:

$$(x_0\, x_\alpha\, x_1) = (x_0\, x_1\, x_\alpha)^2$$

$$(x_0\, x_\alpha\, x_\beta) = (x_0\, x_1\, x_\alpha)^2\, (x_0\, x_1\, x_\beta)$$

$$(x_1\, x_\alpha\, x_\beta) = (x_0\, x_1\, x_\alpha)\, (x_0\, x_1\, x_\beta)^2$$

$$(x_\alpha\, x_\beta\, x_\gamma) = (x_0\, x_1\, x_\alpha)\, (x_0\, x_1\, x_\gamma)\, (x_0\, x_1\, x_\beta)\, (x_0\, x_1\, x_\alpha)\, (x_0\, x_1\, x_\gamma).$$

3. De substituties n°. 1, 2, 7, 8, 17, 18, 23, 24 der symmetrische groep van vier letters, n. l. de substituties

$$s_0 = 1 \qquad s_1 = (x_2 x_3) \qquad s_2 = (x_0 x_1) \qquad s_3 = (x_0 x_1)(x_2 x_3)$$

$$s_4 = (x_0 x_2)(x_1 x_3) \quad s_5 = (x_0 x_2 x_1 x_3) \quad s_6 = (x_0 x_3 x_1 x_2) \quad s_7 = (x_0 x_3)(x_1 x_2)$$

vormen ook eene groep, zooals uit onderstaande tafel van vermenigvuldiging te zien is. Het product van s_i en s_k staat in de horizontale rij, die met s_i en de vertikale kolom, die met s_k begint:

s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
s_1	s_0	s_3	s_2	s_5	s_4	s_7	s_6
s_2	s_3	s_0	s_1	s_6	s_7	s_4	s_5
s_3	s_2	s_1	s_0	s_7	s_6	s_5	s_4
s_4	s_6	s_5	s_7	s_0	s_2	s_1	s_3
s_5	s_7	s_4	s_6	s_1	s_3	s_0	s_2
s_6	s_4	s_7	s_5	s_2	s_0	s_3	s_1
s_7	s_5	s_6	s_4	s_3	s_1	s_2	s_0

4. De machten van eene zelfde substitutie s vormen blijkbaar ook eene groep, want $s^p.\ s^q = s^{p+q}$.

Deze groep heet eene *cyclische groep*, als s eene circuculaire substitutie is De substituties

$s_1 = (x_0x_1x_2x_3x_4x_5)$, $s_2 = (x_0x_2x_4)(x_1x_3x_5)$, $s_3 = (x_0x_3)(x_1x_4)(x_2x_5)$,

$s_4 = (x_0x_4x_2)(x_1x_5x_3)$, $s_5 = (x_0x_5x_4x_3x_2x_1)$ en $s_0 = 1$

vormen eene cyclische groep, omdat zij de achtereenvolgende machten zijn van de eerste substitutie.

§ 40. Twee groepen kunnen, hoe verschillend zij ook schijnen, in de voornaamste eigenschappen overeenstemmen, wanneer het mogelijk is de substituties der eene groep zóó te laten overeenkomen met die der andere groep, dat het product van twee substituties der eene groep tot overeenkomstige substitutie der andere groep heeft het product van de met die twee overeenkomstige substituties der andere groep.

Men noemt in dit geval de twee groepen *isomorf.*

De cyclische groep van 't laatste voorbeeld is b.v. isomorf met deze groep

$\sigma_1 = (x_0\,x_1)(x_2\,x_3\,x_4)$ $\sigma_2 = (x_2\,x_4\,x_3)$ $\sigma_3 = (x_0\,x_1)$

$\sigma_4 = (x_2\,x_3\,x_4)$ $\sigma_5 = (x_0\,x_1)(x_2\,x_4\,x_3)$ $\sigma_0 = 1$

waarvan ook alle substituties de achtereenvolgende machten zijn van σ_1.

Deze isomorfie is eene *holoëdrische* isomorfie of eene isomorfie éen aan éen. Het is echter ook mogelijk, dat met elke substitutie van de éene groep meer substituties van de andere overeenkomen. In dat geval spreekt men van meriëdische isomorfie.

§ 41. Bij sommige groepen is het mogelijk eene substitutie aan te wijzen, die eene willekeurige letter door eene willekeurige vervangt; bij andere is dit niet voor elk geval mogelijk. In het eerste geval heet de groep *transitief,* [1]) in het tweede geval *intransitief.* De symmetrische groep is natuurlijk transitief. Zoo ook de groep van 8 substituties, die als derde voorbeeld in § 39 genoemd is, want x_0 wordt in x_0 overgevoerd door s_0

---

[1]) Het begrip transitiviteit is afkomstig van RUFFINI.

en s_1, in x_1 door s_2 en s_3, in x_2 door s_4 en s_5 en in x_3 door s_6 en s_7. En als één element in alle andere kan worden overgevoerd, is het ook mogelijk elk element in elk ander over te voeren. Ook de cyclische groep in § 39, 4° is transitief. Daarentegen is de groep van § 40 intransitief, want x_0 kan alleen in x_0 en x_1 overgevoerd worden, maar niet in x_2, x_3, x_4.

§ 42. Is eene groep transitief, dan is het soms wel, soms niet mogelijk de elementen, waarop geopereerd wordt, op eene eigenaardige wijze in te deelen. Nemen we als voorbeeld de cyclische groepen, die de machten zijn van cyclische substituties van 5 en 6 elementen:

$$s_0 = 1 \quad s_1 = (x_0\, x_1\, x_2\, x_3\, x_4) \quad s_2 = (x_0\, x_2\, x_4\, x_1\, x_3)$$

$$s_3 = (x_0\, x_3\, x_1\, x_4\, x_2) \quad s_4 = (x_0\, x_4\, x_3\, x_2\, x_1)$$

en: $s_0 = 1 \quad s_1 = (x_0\, x_1\, x_2\, x_3\, x_4\, x_5) \quad x_2 = (x_0\, x_2\, x_4)(x_1\, x_3\, x_5)$

$$s_3 = (x_0 x_3)(x_1 x_4)(x_2 x_5) \quad s_4 = (x_0 x_4 x_2)\,(x_1 x_5 x_3) \quad x_5 = (x_0 x_5 x_4 x_3 x_2 x_1).$$

Bij de laatste groep kunnen de elementen in 2 stellen verdeeld worden x_0, x_2, x_4 en x_1, x_3, x_5 zóó, dat de substituties der groep, òf de elementen van elk stel onderling omzetten òf de elementen van één stel alle omzetten in de elementen van een ander stel: de substituties s_0, s_2, s_4 verwisselen onderling de elementen van elk stel, de substituties s_1, s_3, s_5 vervangen de elementen van het eene stel door elementen van het andere stel. Zulk eene groep heet *imprimitief;* daarentegen heet de cyclische groep van 5 letters, waarbij zulk eene indeeling der elementen in stellen niet mogelijk is, *primitief.* Over primitiviteit en imprimitiviteit [1]) kan alleen sprake zijn bij transitieve groepen, daar het eerst zeker moet zijn, dat elk element door elk ander element kan worden vervangen.

§ 43. Eene groep g, waarvan alle substituties voorkomen in eene andere groep G, die er nog andere bevat, heet

---

[1]) Deze begrippen zijn te vinden bij RUFFINI.

eene *ondergroep* [1]) van G. De alterneerende groep is b.v. eene ondergroep van de symmetrische groep; de groep van 8 substituties in § 39, 3 is eene ondergroep van de symmetrische groep van 4 letters, die uit 24 substituties bestaat. Eene cyclische groep, die uit de machten van eene substitutie s bestaat, is eene ondergroep van elke groep, die de substitutie s bevat, als zij ten minste nog meer substituties bevat dan de machten van s. De identische substitutie is op zich zelve eene ondergroep van elke andere groep.

§ 44. De orde van eene ondergroep g is altijd deelbaar op de orde van de groep G [2]).

Laten, om het te bewijzen,

$$s_0 \quad s_1 \quad s_2 \quad \ldots\ldots \quad s_{n-1}$$

de substituties zijn van de ondergroep g van de orde n, terwijl m de orde is van de groep G. Is dan σ_1 eene substitutie van G, die niet in g voorkomt, dan komen de substituties

$$s_0\sigma_1 \quad s_1\sigma_1 \quad s_2\sigma_1 \quad \ldots\ldots \quad s_{n-1}\sigma_1 \qquad (\alpha)$$

in G, maar niet in g voor, want was $s_i\sigma_1 = s_k$ dan zou $\sigma_1 = s_i^{-1} s_k$ zijn en dus in g voorkomen.

Is met deze substituties de groep G niet uitgeput, maar komt er nog eene substitutie σ_2 in voor, dan zullen

$$s_0\sigma_2 \quad s_1\sigma_2 \quad s_2\sigma_2 \quad \ldots\ldots \quad s_{n-1}\sigma_2 \qquad (\beta)$$

weer wel in G, maar niet in g, noch in de rij (α) voorkomen. Was b.v. $s_i\sigma_2 = s_k\sigma_1$, dan zou $\sigma_2 = s_i^{-1} s_k\sigma_1$ zijn, dus zou σ_2 in (α) voorkomen, hetgeen in strijd is met hetgeen we verondersteld hebben. Zijn met de groep g en de rijen (α) en β) de substituties van G niet uitgeput, dan kan men de redeneering op dezelfde wijze voortzetten en zoo aantoonen, dat de substituties van G ge-

[1]) WEBER spreekt van een *deeler* eener groep.
[2]) Stelling van LAGRANGE. Zie JORDAN, blz. 25.

rangschikt kunnen worden in rijen, die elk n substituties bevatten. n is derhalve een deeler van m. Het quotient $\frac{m}{n}$ is een geheel getal ν: 't wijst aan welk deel van het totale getal substituties van G in g voorkomt en heet de *index* van de ondergroep g in de groep G.

§ 45. Gevolgen. 1. Daar elke groep van m letters eene ondergroep is van de symmetrische groep van m letters, is de orde van elke groep van m letters een deeler van $m!$

2. Daar de orde van elke substitutie tegelijk de orde is van de groep uit de machten dezer substitutie bestaande, is de orde van elke substitutie een deeler van de orde der groep, waartoe de substitutie behoort.

3. Is de orde eener groep een priemgetal p, dan kan de groep niet anders bevatten dan de eenheid en substituties der orde p. Maar, als zij ééne substitutie der orde p bevat, is het totale aantal substituties uitgeput door de machten van deze: de groep is dus cyclisch.

4. Is G transitief, dan vormen alle substituties, die x_0 in x_0 overvoeren, dus onveranderd laten eene ondergroep g. Schrijft men deze in de eerste rij, dan zullen, als σ_1 het element x_0 in x_1 overvoert, alle substituties der rij (α) hetzelfde doen en geen andere substitutie zal x_0 in x_1 overvoeren, want deed $s_i \sigma_k$ het, dan zou $s_i \sigma_k \sigma_1^{-1}$ 't element x_0 onveranderd laten en dus tot g behooren. Maar dit kan niet, want uit $s_i \sigma_k \sigma_1^{-1} = s_j$ zou volgen $\sigma_k = s_i^{-1} s_j \sigma_1$, dus σ_k zou tot de rij (α) behooren.

gσ_i bevat dus alle substituties, die x_0 in een zelfde element overvoeren: het aantal rijen is dus gelijk aan 't aantal elementen en de orde eener transitieve groep is deelbaar door haar graad.

§ 46. Men schrijft symbolisch:

$$G = g + g\sigma_1 + g\sigma_2 + \dots + g\sigma_{\nu-1} \qquad [1]$$

[1]) Deze schrijfwijze is van GALOIS. Oeuvres, bldz. 26.

g is eene groep, $g\,\sigma_i$ niet want deze rijen bevatten niet de identische substitutie. De substituties der groep kunnen ook anders in rijen geschikt worden, zóó n.l. als symbolisch wordt voorgesteld door

$$G = g + \tau_1 g + \tau_2 g + \ldots + \tau_{\nu-1} g.$$

§ 47. Het omgekeerde van de stelling in § 44 is door CAUCHY [1]) bewezen: is de orde m eener groep G deelbaar door een priemgetal p, dan bevat G eene ondergroep van de orde p. SYLOW [2]) heeft de stelling uitgebreid: hij bewijst, dat eene groep G, welker orde door p^α (p = priemgetal) deelbaar is, eene ondergroep van de orde p^α bevat.

§ 48. Vormen de substituties

$$s_1 = 1\,,\ s_1\,,\ s_2\,,\ \ldots\ s_{n-1} \qquad (1)$$

eene ondergroep g in G, dan kan men al deze substituties door eene zelfde substitutie σ_1 van G, die niet in g voorkomt, transformeeren (§ 15) tot

$$\sigma_1^{-1} s_0 \sigma_1 = 1,\ \ \sigma_1^{-1} s_1 \sigma_1\,,\ \ \sigma_1^{-1} s_2 \sigma_1\,, \ldots\ldots\ \sigma_1^{-1} s_{n-1} \sigma_1. \quad (2)$$

Deze substituties vormen eene groep, want

$$\sigma_1^{-1} s_i \sigma_1 \,.\, \sigma_1^{-1} s_j \sigma_1 = \sigma_1^{-1} s_i s_j \sigma_1 = \sigma_1^{-1} s_k \sigma_1$$

als $s_i s_j = s_k$ is. Deze groep stellen we voor door $\sigma_1^{-1} g \sigma_1$.

Alle substituties van de rij $g\,\sigma_1$

$$s_0 \sigma_1\,,\ s_1 \sigma_1\,,\ s_2 \sigma_1 \ldots\ldots s_{n-1} \sigma_1$$

transformeeren de groep g in dezefde groep $\sigma_1^{-1} g \sigma_1$, want

$$(s_i \sigma_1)^{-1} s_j (s_i \sigma_1) = \sigma_1^{-1} s_1^{-1} s_j s_i \sigma_1 = \sigma_1^{-1} s_l \sigma_1$$

als de substitutie $s_1^{-1} s_j s_i$ van g door s_l wordt voorgesteld.

---

[1]) Exercices d'analyse et de physique mathématique, t. III, bldz. 250.
[2]) Mathematische Annalen V, bldz. 584.

Daar geen twee substituties s_j dezelfde substitutie door transformatie kunnen opleveren, zal de groep, die uit g ten gevolge van transformatie door σ_1 ontstaat, dezelfde zijn als die, welke met behulp van $s_i\sigma_1$ ontstaat.

Op dezelfde wijze transformeert elke substitutie der rij $g\sigma_2$ de groep g in $\sigma_2^{-1} g \sigma_2$. Komt dus in G eene ondergroep g voor van den index ν, dan komen in die groep ook voor de ondergroepen

$$g_1 = \sigma_1^{-1} g \sigma_1, \; g_2 = \sigma_2^{-1} g \sigma_2, \ldots \; g_{\nu-1} = \sigma_{\nu-1}^{-1} g \sigma_{\nu-1}$$

welker substituties alle gelijkvormig zijn met die van g.

Daarom zegt men ook, dat de groepen gelijkvormig zijn.

Verder heeten de ondergroepen g, $g_1, \ldots g_{\nu-1}$ *gelijkstaande ondergroepen* [1]) in G.

g is in deze verzameling ondergroepen in niets onderscheiden van $g_1, \ldots g_{\nu-1}$: men kan evengoed van eene andere ondergroep g_i uitgaan en daarbij door transformatie de gelijkstaande ondergroepen vormen; men vindt dan hetzelfde stel g, g_1, g_2, ... $g_{\nu-1}$.

§ 49. Voorbeeld. De symmetrische groep G van 4 letters (§ 39, 1) bevat de ondergroep g (voorbeeld 3 § 39):

$$s_0 = 1 \qquad s_1 = (x_2x_3) \qquad s_2 = (x_0x_1) \qquad s_3 = (x_0x_1)(x_2x_3)$$

$$s_4 = (x_0x_2)(x_1x_3) \quad s_5 = (x_0x_2x_1x_3) \quad s_6 = (x_0x_3x_1x_2) \quad s_7 = (x_0x_3)(x_1x_2)$$

Neemt men $\sigma_1 = (x_1\, x_2\, x_3)$ en $\sigma_2 = (x_1\, x_3)$, dan worden de rijen $g\sigma_1$ en $g\sigma_2$:

$$g\sigma_1 = (x_1 x_2 x_3), \quad (x_1 x_2), \quad (x_0 x_2 x_3 x_1), \quad (x_0 x_2 x_1),$$
$$(x_0 x_3 x_2), \quad (x_0 x_3), \quad (x_0 x_1 x_3 x_2), \quad (x_0 x_1 x_3).$$
$$g\sigma_2 = (x_1 x_3), \quad (x_1 x_3 x_2), \quad (x_0 x_3 x_1), \quad (x_0 x_3 x_2 x_1),$$
$$(x_0 x_2), \quad (x_0 x_2 x_3), \quad (x_0 x_1 x_2). \quad (x_0 x_1 x_2 x_3).$$

Transformeert men alle substituties van g door eene

[1]) In Duitsche werken: gleichberechtigte Untergruppen.

substitutie van de rij $g\sigma_1$ en door eene van de rij $g\sigma_2$ b.v. door $(x_1 x_2)$ en $(x_1 x_3)$, dan vindt men de met g gelijkstaande groepen:

$$g_1 = \sigma_1^{-1} g \sigma_1: \quad s_0' = 1 \quad s_1' = (x_1 x_3) \quad s_2' = (x_0 x_2) \quad s_3' = (x_0 x_2)(x_1 x_3)$$
$$s_4' = (x_0 x_1)(x_2 x_3) \quad s_5' = (x_0 x_1 x_2 x_3) \quad s_6' = (x_0 x_3 x_2 x_1) \quad s_7' = (x_0 x_3)(x_1 x_2)$$
$$g_2 = \sigma_2^{-1} g \sigma_2: \quad s_0'' = 1 \quad s_1'' = (x_1 x_2) \quad s_2'' = (x_0 x_3) \quad s_3'' = (x_0 x_3)(x_1 x_2)$$
$$s_4'' = (x_0 x_2)(x_1 x_3) \quad s_5'' = (x_0 x_2 x_3 x_1) \quad s_6'' = (x_0 x_1 x_3 x_2) \quad s_7'' = (x_0 x_1)(x_2 x_3)$$

§ 50. Deze gelijkstaande groepen, wier gezamenlijk aantal substituties gelijk is aan het totale aantal substituties van G, bevatten samen niet *alle* substituties van G, want de identische substitutie komt b.v. al ν malen voor. De groepen g, g_1, g_2, ... bevatten dus zeker gemeenschappelijke substituties. Het kan zelfs gebeuren, dat zij volmaakt met elkaar overeenstemmen: in dat geval zegt men, dat g eene *alleenstaande ondergroep* [1]) van G is.

Voorbeelden. 1. Eene even substitutie blijft door transformatie van welke substitutie ook, altijd eene even substitutie. Elke ondergroep, die met de alterneerende gelijk staat in de symmetrische groep, bevat dus ook alle even substituties. De alterneerende groep is dus eene alleenstaande groep in de symmetrische groep

2. Elke ondergroep van eene cyclische groep

$$s_0 = 1, \; s, \; s^2, \; \ldots . \; s^{n-1}$$

is eene alleenstaande groep. Want transformeert men b.v. s^i door eenig andere substitutie s^α, dan vindt men $s^{-\alpha} s^i s^\alpha = s^i$: er ontstaat dus geen andere substitutie.

§ 51. Zijn de gelijkstaande groepen

$$g, \; g_1, \; g_2 \; \cdots\cdots\cdots \; g_{\nu-1}$$

---

[1]) In Duitsche werken: ausgezeichnete Untergruppe: bij WEBER: Normaltheiler.

niet identisch, dan vormen de aan al deze groepen gemeenschappelijke substituties eene groep, want het product van twee dezer substituties moet zoowel in g, als in g_1, ... $g_{\nu-1}$ voorkomen en behoort dus tot de verzameling. Maar bovendien is deze groep in G eene alleenstaande groep, want wanneer alle gelijkstaande ondergroepen

$$g, \; g_1, \; g_2, \; \ldots\ldots \; g_{\nu-1}$$

door eene zelfde substitutie τ van G getransformeerd worden, dan gaan zij over in dezelfde reeks gelijkstaande groepen in andere volgorde. Eene substitutie σ, die aan alle groepen g, ... g_{-1} gemeen is, zal dus door transformatie overgaan in eene substitutie, die nog in alle gelijkstaande groepen voorkomt. Derhalve is de grootstgemeene ondergroep der gelijkstaande ondergroepen g, ... $g_{\nu-1}$ eene alleenstaande groep in G.

In het voorbeeld van § 49 vinden we als de grootstgemeene ondergroep van g, g_1, g_2

$$s_0 = 1 \quad s_3 = (x_0\, x_1)(x_2\, x_3) \quad s_4 = (x_0\, x_2)(x_1\, x_3) \quad s_7 = (x_0\, x_3)(x_1\, x_2).$$

Men overtuigt er zich gemakkelijk van, dat deze substituties eene groep vormen en dat de groep alleenstaande is in de groep G van alle substituties van 4 letters. 't Is de viergroep van KLEIN. [1])

§ 52. We geven nu nog een paar voorbeelden, die we voor latere toepassingen noodig hebben: ze zullen doen zien, hoe het mogelijk is, groepen te vormen, die vooraf bepaalde eigenschappen bezitten.

Zij vooreerst gevraagd naar de grootste groep van p letters ($p =$ priemgetal), waarvan de cyclische groep van p letters eene alleenstaande ondergroep is [2]).

Een cyclische groep van een ondeelbaar aantal letters

---

[1]) KLEIN. Ikosaëder, bldz. 12.

[2]) GALOIS. Oeuvres, bldz. 47.
BOLZA. American Journ. of Math. XIII, bldz 130

p bestaat uit de machten van $(x_0\ x_1\ x_2 \ldots . x_{p-1})$ of in andere notatie, van $[z \quad z+1]$ mod p. De groep bevat dus de substituties

$$[z \quad z+c] \quad \text{mod } p \quad c=0,\ 1,\ 2, \ldots\ p-1.$$

Zij $t=[z \quad \varphi(z)]$ eene substitutie van de gezochte groep G. Transformeert men $s=[z \quad z+1]$ door t, dan vindt men:

$$t^{-1}\, s\, t=[\varphi(z) \quad \varphi(z+1)]$$

Deze substitutie moet tot de cyclische groep behooren, derhalve

$$[\varphi(z) \quad \varphi(z+1)]=[z \quad z+c] \text{ of } =[\varphi(z) \quad \varphi(z)+c].$$

Daaruit volgt

$$\varphi(z+1) \equiv \varphi(z)+c \quad (\text{mod } p)$$

voor $z=0,\ 1, \ldots .\ p-1$. Derhalve:

$$\varphi(1) \equiv \varphi(0)+c$$

$$\varphi(2) \equiv \varphi(1)+c \equiv \varphi(0)+2c$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\varphi(i) \equiv \varphi(i-1)+c \equiv \varphi(0)+ic.$$

Stelt men $\varphi(0)=b$, dan vindt men dus

$$\varphi(z) \equiv cz+b \quad (\text{mod } p)$$

voor $c=1,\ 2, \ldots .\ p-1$ en $b=0,\ 1,\ 2, \ldots .\ p-1$.

De grootste groep, die de cyclische groep van p letters als alleenstaande ondergroep bevat, bestaat dus uit $p(p-1)$ substituties. Zij heet de *metacyclische groep.*

De cyclische substituties er van vindt men door $c=1$ te stellen. Verschilt c van 1, dan is er onder alle substituties waarvoor c dezelfde waarde heeft, éene, waarin éen element onveranderd blijft, n. l. dat, welks index voldoet aan de congruentie $cz+b \equiv z$ (mod p).

§ 53. Zij als een tweede voorbeeld gevraagd naar de grootste transitieve groep G van p elementen (p = priem getal) waarvan geen enkele substitutie (de identiteit uit-

gezonderd) meer dan één element onveranderd laat. [1])

Elke substitutie s zal regelmatig moeten zijn, want was i het kleinste aantal elementen, dat in een cyclus voorkomt, dan zou s^i i elementen onverplaatst laten zonder de identiteit te zijn. De groep kan dus, behalve de identiteit, niet anders bevatten dan cyclische substituties van p elementen en regelmatige substituties van $p—1$ elementen.

Alle substituties, die x_0 onveranderd laten, vormen eene groep g. Er zullen evenveel substituties zijn, die x_i onveranderd laten, want, als t eene substitutie voorstelt, die x_0 in x_i overvoert (die is er, omdat de groep transitief is), dan zal de groep, die x_0 onveranderd laat, als zij door t getransformeerd wordt, overgaan in de groep, die x_i onveranderd laat en omgekeerd zal elke substitutie, die x_i onveranderd laat, als zij door t^{-1} getransformeerd wordt, overgaan in eene substitutie, die x_0 onveranderd laat.

Bij de groep g zullen de gelijkstaande ondergroepen $g_1, \ldots\ldots g_{p-1}$ te vinden zijn, die resp. de elementen $x_1, \ldots . x_{p-1}$ onveranderd laten. De groep g moet dan tot index p hebben en dus, als m ook de orde van G voorstelt, $\frac{m}{p}$ substituties bevatten. Hierbij is de identiteit en dus nog $\frac{m}{p} - 1$ substituties van $p - 1$ letters. In 't geheel zijn er dus $p\left(\frac{m}{p} - 1\right) = m - p$ substituties van $p - 1$ letters

Rekent men nog op de identiteit, dan blijkt het, dat er $m - (m - p) - 1 = p - 1$ substituties van p letters aanwezig zijn.

Eéne cyclische substitutie van p letters doet door machtsverheffing $p - 1$ van die substituties ontstaan (behalve de identiteit): met de machten van ééne enkele

[1]) Weber. Algebra I, § 180.

cyclische substitutie van p letters zijn dus de beschikbare cyclische substituties van p letters uitgeput. Deze substituties vormen derhalve eene ondergroep van G en, daar uit elke cyclische substitutie van p letters door transformatie eene dergelijke substitutie ontstaat, vormen de cyclische substituties van p letters in G eene alleenstaande ondergroep. Maar dan leert de vorige § ons, dat de groep G de metacyclische groep moet zijn.

§ 54. Rangschikken we de substituties van de metacyclische groep nu nog volgens § 44. Nemen we in de eerste rij de cyclische ondergroep der orde p, die gevonden wordt door $c = 1$ te stellen en nemen we voor de substituties σ_1, $\sigma_2 \ldots\ldots \sigma_{p-2}$ de volgende:

$$\sigma_1 = [z \quad 2z],\ \sigma_2 = [z \quad 3z], \ldots\ldots \sigma_{p-2} = [z \quad (p-1)z]$$

alles mod. p, dan wordt de rangschikking:

$$\begin{array}{lll} [z \quad z] \quad , & [z \quad z+1], \ldots\ . & [z \quad z+p-1] \\ [z \quad 2z] \quad , & [z \quad 2z+1], \ldots\ldots & [z \quad 2z+p-1] \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ [z \ (p-1)z], & [z \ (p-1)z+1], \ldots\ldots & [z \ (p-1)z+p-1]. \end{array}$$

Men kan met behoud van de eerste rij de rijen nog anders op elkaar laten volgen. Is toch g eene primitieve wortel (mod. p) d. w. z. is g zóo, dat de getallen g^0, g^1, $g^2, \ldots\ldots g^{p-2}$ bij deeling door p de resten $1, 2, 3, \ldots\ldots p-1$ in andere volgorde geven, dan kan men de σ's nemen in de volgorde $\sigma_0 = 1, \sigma_g, \sigma_{g^2}, \sigma_{g^3}, \ldots\ldots \sigma_{g^{p-2}}$ (mod. p).

De σ's vormen dan ook eene cyclische groep van de orde $p-1$.

HOOFDSTUK III.

Rationale functiën en substitutiegroepen.

§ 55. Beschouwen we nu de elementen $x_0, x_1, \ldots . x_{m-1}$, waarop in het vorige hoofdstuk substituties zijn uitgevoerd, als onafhankelijk veranderlijke grootheden, die de wortels zijn van eene m^{de}-machtsvergelijking

$$x^m - c_1 x^{m-1} + c_2 x^{m-2} - \ldots . \pm c_m = 0.$$

Onderstellen we al deze wortels verschillend.

Is het om de oplossing dezer vergelijking te doen, dan zijn de symmetrische functiën $c_1, c_2, \ldots . c_m$ der wortels gegeven, terwijl de wortels, of functiën van de wortels, waaruit de wortels zelve gevonden kunnen worden, in $c_1, \ldots . c_m$ moeten worden uitgedrukt.

§ 56. Elke rationale functie van de wortels blijft door een aantal substituties tusschen de grootheden $x_0, \ldots x_m$ onveranderd.

B. v. de functie van de 4 grootheden x_0, x_1, x_2, x_3, $x_0 x_1 + x_2 x_3$ blijft onveranderd, wanneer men haar onderwerpt aan de substituties

$$s_0 = 1 \qquad s_1 = (x_2 x_3) \qquad s_2 = (x_0 x_1) \qquad s_3 = (x_0 x_1)(x_2 x_3)$$

$$s_4 = (x_0 x_2)(x_1 x_3) \quad s_5 = (x_0 x_2 x_1 x_3) \quad s_6 = (x_0 x_3 x_1 x_2) \quad s_7 = (x_0 x_3)(x_1 x_2).$$

De functie verandert echter, wanneer zij onderworpen wordt aan eene andere substitutie der vier letters.

We beschouwen alleen *rationale* functiën, omdat van de veranderingen van irrationale functiën niets te zeggen is, b. v. van de functie $x_0 - x_1$ kan men zeggen, dat zij van teeken verandert, als men x_0 en x_1 verwisselt; of de functie $\sqrt{x_0^2 - 2x_0x_1 + x_1^2}$ door deze verwisseling van teeken verandert, is echter niet uit te maken.

§ 57. Alle substituties, die eene rationale functie der grootheden $x_0, \ldots x_{m-1}$ onveranderd laten, vormen eene groep, want, wordt φ onveranderd gelaten door de substituties s_1 en s_2, dan kan men eerst s_1 en daarna s_2 op φ toepassen, zonder dat φ verandert: φ is dus onveranderd gebleven door $s_1 s_2$, d. w. z. als s_1 en s_2 behooren tot de substituties, die φ onveranderd laten, behoort $s_1 s_2$ er ook toe.

Eene rationale functie, die door *elke* substitutie verandert, maakt geen uitzondering op den regel: de substitutie 1 alleen laat haar onveranderd en deze substitutie vormt eene groep op zich zelve.

Voorbeelden. 1. Elke symmetrische functie van $x_0, \ldots x_{m-1}$ blijft onveranderd door alle substituties der m grootheden. Al deze substituties vormen samen de symmetrische groep.

2. De alterneerende functie der m grootheden

$$(x_0-x_1)(x_0-x_2)\ldots(x_0-x_{m-1})(x_1-x_2)\ldots(x_1-x_{m-1})\ldots(x_{m-2}x_{m-1})$$

verandert van teeken, als zij aan eene transpositie wordt onderworpen . Zij blijft dus onveranderd door alle substituties, die als een even aantal transposities geschreven kunnen worden d. i. door alle substituties van de alterneerende groep.

3. De functie $x_0x_1 + x_2x_3$ blijft onveranderd door de groep van 8 substituties, die wij in de vorige § hebben neergeschreven en in § 39, 3 behandeld.

4. De functie

$$(x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots \varepsilon^{m-1} x_{m-1})^m$$

waarin ε eene complexe m^{de}-machtswortel der eenheid voorstelt, blijft onveranderd door de cyclische substitutie $(x_0 x_1 \ldots . x_{m-1})$ en door al hare machten, dus door de cyclische groep. Door elke andere substitutie verandert zij.

§ 58. Omgekeerd zijn ook bij elke groep rationale functiën te vinden, die door de substituties der groep en door geen andere substituties onveranderd gelaten worden.

Daartoe kan men de functie [1])

$$V = \lambda_0 x_0 + \lambda_1 x_1 + \ldots . \lambda_{m-1} x_{m-1}$$

vormen, waarin $\lambda_0, \lambda_1, \ldots . \lambda_{m-1}$ verschillende constanten voorstellen en op deze functie de substituties $s_0 = 1, s_1, \ldots .$ $, \ldots s_{n-1}$ der groep g toepassen. Gaat V daardoor over in $V, V_1, \ldots . V_{n-1}$, dan zal elke symmetrische functie dezer grootheden door de substituties van g en door geen enkele andere substitutie onveranderd blijven.

Men zegt, dat eene functie en de substitutiegroep, waardoor zij onveranderd blijft, bij elkaar behooren.

§ 59. Beschouwen we eene groep G, eene ondergroep g van den index ν en eene functie φ, die bij g behoort. Schrijven we dan, zooals in § 44 de substituties van G in rijen, waarvan de eerste door de substituties van g gevormd wordt:

$$\begin{array}{lllll} s_0 = 1, & s_1, & s_2, & \ldots . & s_{n-1} \\ s_0 \sigma_1, & s_1 \sigma_1, & s_2 \sigma_1, & \ldots . & s_{n-1} \sigma_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ s_0 \sigma_{\nu-1}, & s_1 \sigma_{\nu-1}, & s_2 \sigma_{\nu-1}, & \ldots . & s_{n-1} \sigma_{\nu-1} \end{array}$$

dan laten alle substituties der eerste rij φ onveranderd; alle substituties der 2de rij voeren φ in dezelfde functie φ_1 over, waarin σ_1 φ overvoert. Evenzoo zullen alle substituties eener andere rij φ in eene en dezelfde functie φ_i overvoeren. En daar het aantal rijen ν is, zal φ door

[1]) GALOIS. Oeuvres bldz 36.

alle substituties van groep G ν verschillende waarden krijgen: $\varphi, \varphi_1, \varphi_2, \ldots . \varphi_{\nu-1}$.

Deze waarden $\varphi, \varphi_1, \ldots \ldots \varphi_{\nu-1}$ heeten toegevoegde functiën van φ in de groep G. Men zegt, dat φ in G ν-waardig is. Het aantal waarden van φ is een deeler van $m!$

Voorbeeld. De functie $x_0 x_1 + x_2 x_3$, die door de acht substituties van de groep g (§ 49) onveranderd blijft, wordt door de rij g σ_1 overgevoerd in $x_0 x_2 + x_1 x_3$ en door de rij g σ_2 in $x_0 x_3 + x_1 x_2$. Deze functie is dus driewaardig in de symmetrische groep.

§ 60. Bij elk der functiën $\varphi, \varphi_1, \ldots \ldots \varphi_{\nu-1}$ behoort eene groep.

Daar $\varphi, \ldots . . \varphi_{\nu-1}$ volmaakt dezelfde functiën zijn van de veranderlijken $x_0, \ldots . . x_{m-1}$, waarbij die veranderlijken alleen telkens in andere volgorde genomen zijn, zijn de groepen, die er bij behooren, zeker gelijksoortige groepen en men overtuigt er zich gemakkelijk van, dat het de gelijkstaande groepen zijn van § 48.

Immers, de functie φ_i ontstaat uit φ door de substitutie σ_i; omgekeerd ontstaat φ uit φ_i door de substitutie σ_i^{-1}.

Past men nu op φ_i achtereenvolgens toe de substitutie σ_i^{-1}, eene substitutie van g en daarna σ_i, dan gaat eerst φ_i over in φ, daarna blijft φ onveranderd en vervolgens gaat φ weer over in φ_i. De functie φ_i blijft dus onveranderd door de groep σ_i^{-1} g σ_i.

Behoort φ dus bij eene ondergroep g van G, dan behooren de toegevoegde functiën $\varphi_1, \varphi_2, \ldots \ldots \varphi_{\nu-1}$ bij de daarmede gelijkstaande ondergroepen

$$\sigma_1^{-1} \mathrm{g}\, \sigma_1, \ \sigma_2^{-1} \mathrm{g}\, \sigma_2 \ldots \ldots \sigma_{\nu-1}^{-1} \mathrm{g}\, \sigma_{\nu-1}.$$

Zijn deze gelijkstaande ondergroepen identiek, zoodat g eene alleenstaande ondergroep is, dan behooren alle toegevoegde functiën $\varphi, \varphi_1 \ldots \ldots \ldots \varphi_{\nu-1}$ bij éene en dezelfde groep.

§ 61. Dat bij eene zelfde groep verschillende functiën

kunnen behooren, is reeds in § 58 gebleken. Tusschen deze functiën heeft LAGRANGE [1]) een merkwaardig verband gevonden: zij zijn rationaal in elkaar uit te drukken.

Zij, om eene eenigszins algemeenere stelling te bewijzen, Φ eene functie, die onveranderd blijft door alle substituties, die de functie φ onveranderd laten en misschien door nog andere substituties. De groep bij φ behoorende is dan eene ondergroep van de groep, die Φ onveranderd laat of deze groep zelve. Alle substituties, die φ in φ_i overvoeren, zullen dus ook Φ in eene zelfde functie overvoeren. Laat φ door alle substituties overgevoerd worden in

$$\varphi,\ \varphi_1, \ldots\ldots \varphi_{\nu-1}$$

en Φ door dezelfde substituties in

$$\Phi,\ \Phi_1, \ldots\ldots \Phi_{\nu-1}$$

dan kunnen er onder deze laatste functiën gelijke voorkomen.

Vorm nu de rationale functie

$$R(\xi) \equiv (\xi - \varphi)(\xi - \varphi_1) \ldots (\xi - \varphi_{\nu-1}) \times$$
$$\times \left(\frac{\Phi}{\xi - \varphi} + \frac{\Phi_1}{\xi - \varphi_1} + \ldots \frac{\Phi_{\nu-1}}{\xi - \varphi_{\nu-1}}\right)$$

eene geheele functie van den graad $\nu - 1$ in ξ, die door alle substituties in zich zelve wordt overgevoerd en die dus eene symmetrische functie van $x_0, x_1, \ldots x_{m-1}$ is.

Stelt men hierin $\xi = \varphi$, dan vindt men als

$$(\xi - \varphi)(\xi - \varphi_1) \ldots\ldots (\xi - \varphi_{\nu-1}) = r(\xi)$$

wordt gesteld

$$R(\varphi) = \Phi \,.\, r'(\varphi) \qquad \text{of}$$

$$\Phi = \frac{R(\varphi)}{r'(\varphi)}$$

d. w. z. Φ is rationaal in φ uit te drukken [2]).

---

[1]) Mémoires de l'Académie de Berlin, 1771.

[2]) WEBER, Algebra I, § 155, 1e druk, 1895.

Alle geheele rationale functiën, die bij eene zelfde groep behooren, kunnen dus over en weer rationaal in elkaar worden uitgedrukt. En elke geheele rationale functie der grootheden $x_0, \ldots . x_{m-1}$ is rationaal uit te drukken in de $m!$-waardige functie V van § 58.

§ 62. Laat nu Φ eene functie zijn, die bij eene groep G behoort en φ eene functie, die behoort bij de ondergroep g, die in G den index ν heeft. Dan is φ ν-waardig in G en de toegevoegde functiën $\varphi, \varphi_1, \ldots . \varphi\ _{-1}$ zullen de wortels zijn van de vergelijking

$$(\xi - \varphi)(\xi - \varphi_1) \ldots . (\xi - \varphi_{\nu-1}) = 0$$

welker coëfficienten door de substituties van G onveranderd blijven: deze coëfficienten zijn dus rationaal in Φ en $c_1, c_2, \ldots . c_m$ uit te drukken.

De ν toegevoegde waarden van φ in G zijn dus de wortels van de ν^{de} machtsvergelijking

$$\xi^{\nu} - R_1 (\Phi, c_1, c_2, \ldots c_m)\ \xi^{\nu-1} + \ldots + R_{\nu} (\Phi, c_1, c_2 \ldots c_m) = 0$$

waarin de R's rationale functiën voorstellen [1]).

§ 63. Beschouwen we nu nog eens LAGRANGE's oplossing van de volledige derdemachtsvergelijking:

$$x^3 + c_1 x^2 + c_2 x + c_3 = 0.$$

(§ 14, vergelijking (41)). De functiën der wortels, die bekend zijn, n. l. c_1, c_2, c_3 behooren bij de symmetrische groep G:

$$s_0 = 1 \qquad s_1 = (x_0\, x_1\, x_2) \qquad s_2 = (x_0\, x_2\, x_1)$$

$$s_3 = (x_0\, x_1) \qquad s_4 = (x_1\, x_2) \qquad s_5 = (x_0\, x_2).$$

LAGRANGE bepaalt nu eerst de functie $(x_0 + \varepsilon\, x_1 + \varepsilon^2 x_2)^3$, waarin ε eene complexe derdemachtswortel der eenheid voorstelt, uit eene vierkantsvergelijking, welker coëfficienten rationaal in de c's zijn. Dit is in overeenstem-

[1]) LAGRANGE. Mém. de Berlin, 1771.

ming met de stelling in de vorige §, want de functie $(x_0 + \varepsilon x_1 + \varepsilon^2 x_2)^3$ blijft onveranderd door de substituties

$$s_0 = 1 \quad s_1 = (x_0\, x_1\, x_2) \quad s_2 = (x_0\, x_2\, x_1)$$

die eene ondergroep van G vormen van den index 2. Daarna bepaalt LAGRANGE de functie $x_0 + \varepsilon x_1 + \varepsilon^2 x_2$, die alleen door de substitutie 1 onveranderd blijft en die dus uit eene derdemachtsvergelijking te vinden is, welker coëfficienten rationaal zijn in $(x_0 + \varepsilon x_1 + \varepsilon^2 x_2)^3$ en de c's. Maar dan is elke functie van de wortels, dus ook de wortels zelve, rationaal uit te drukken in deze functie $x_0 + \varepsilon x_1 + \varepsilon^2 x_2$.

§ 64. Aan dit eenvoudige voorbeeld is te zien, hoe de gang der bewerkingen zal moeten zijn bij de oplossing der m^{de}-machtsvergelijking

$$x^m - c_1 x^{m-1} + c_2 x^{m-2} \ldots\ldots = 0. \qquad (1)$$

De functiën $c_1, c_2, \ldots. c_m$ der wortels, die bij de symmetrische groep G behooren, zijn bekend. Zondert men uit de groep G eene ondergroep g af van den index ν, dan kan men eene functie φ, die bij g behoort, uit eene ν^{de}-machtsvergelijking bepalen, welker coëfficienten rationale functiën der c' s zijn.

In de groep g kan men weer zoeken eene ondergroep g' met aanwijzer ν': eene functie φ' die bij deze ondergroep behoort, kan men dan vinden uit eene vergelijking van den graad ν', welker coëfficienten rationaal in φ en de c's zijn uit te drukken. In g' kan men weer eene groep g'' vinden van den aanwijzer ν'', en eene functie φ'' bepalen uit eene vergelijking van den graad ν'' met bekende coëfficienten Zoo voortgaande kan men eindelijk eene functie vinden, die bij de groep 1 behoort en waarin de wortels rationaal zijn uit te drukken.

§ 65. De oplossing van de vergelijking is dus teruggebracht tot het oplossen der resolventen, waaruit de functiën $\varphi, \varphi', \varphi'', \ldots..$ gevonden kunnen worden.

Zal echter de vergelijking (1) opgelost kunnen worden door worteltrekkingen, dan zijn de hulpfunctiën, die bepaald moeten worden vóor men eene uitdrukking voor de wortels vindt, door worteltrekking te bepalen: die functiën zijn dus wortels van binomische vergelijkingen.

We staan dus nu voor de vraag: onder welke omstandigheden zal de ν^{de}-graads resolvente voor φ (§ 62) eene binomische vergelijking worden?

De wortels eener binomische vergelijking verschillen alleen in een constanten factor (een complexen eenheidswortel): die toegevoegde functiën blijven dus door dezelfde substituties onveranderd. De gelijkstaande groepen van § 60 zijn in dit geval identiek: de ondergroep, waarbij de functie behoort, is eene alleenstaande ondergroep. Derhalve: zal de functie φ, die bij de ondergroep g in eenige groep G behoort, uit eene binomische vergelijking gevonden kunnen worden, dan moet g eene alleenstaande ondergroep in G zijn.

Daar de worteltrekkingen, die bij de oplossing eener vergelijking uitgevoerd moeten worden, altijd terug te brengen zijn tot worteltrekkingen, waarvan de exponent een ondeelbaar getal is, zal voor de algebraïsche oplosbaarheid op de wijze, die hier geschetst is, vereischt worden, dat de groep g, die bij de functie φ behoort, eene alleenstaande ondergroep is in G, waarvan de aanwijzer een priemgetal is.

§ 66. Omgekeerd blijkt deze voorwaarde ook voldoende te zijn: als g een alleenstaande ondergroep is van eene groep G van ondeelbaren index, is bij g altijd eene functie te vinden, die uit eene binomische vergelijking te bepalen is. Is toch φ eene willekeurige bij g behoorende functie en zijn φ, φ_1, ... $\varphi_{\nu-1}$ de toegevoegde functiën in G, dan blijven al deze functiën onveranderd door alle substituties van g, omdat de met g gelijkstaande ondergroepen van G met g identiek zijn. De functie

$$\chi = \varphi + \varepsilon\varphi_1 + \varepsilon^2\varphi_2 + \ldots\ldots \varepsilon^{\nu-1}\varphi_{\nu-1}$$

waarin ε eene complexe ν^{de}-machtswortel der eenheid is, blijft dus ook onveranderd voor de substituties van g.

Gaan we na, wat deze functie χ wordt, als wij er alle substituties van G op toepassen; denken wij daarbij die substituties gerangschikt in de rijen van § 44.

De substituties $s_0 = 1$, $s_1, s_2, \ldots\ldots s_{n-1}$ van g laten χ onveranderd. σ_1 voert alle φ's in dezelfde grootheden in andere volgorde over; hetzelfde doen alle substituties gσ_1: χ wordt daardoor overgevoerd in χ_1. Evenzoo voeren alle substituties gσ_2 de functie χ in eene zelfde functie χ_2 over. Zoo voortgaande blijken alle mogelijke substituties van G, uitgevoerd op de grootheden

$$\varphi, \varphi_1, \varphi_2, \ldots\ldots \varphi_{\nu-1}$$

verwisselingen van deze grootheden ten gevolge te hebben.

Deze φ-substituties vormen eene groep Γ, die isomorf is met de groep G en wel komt met elke n substituties van G éene substitutie van Γ overeen.

De groep Γ tusschen de ν grootheden $\varphi, \ldots\ldots \varphi_{\nu-1}$ bevat ν substituties; maar daar ν hier ondeelbaar ondersteld wordt, is de groep Γ (§ 45, 3) cyclisch. χ^ν (§ 57, 4) blijft dus onveranderd door alle substituties der groep Γ (als tenminste de volgorde der φ's in χ behoorlijk gekozen is), dus ook door alle substituties der groep G. χ is dus rationaal in Φ en de c's uit te drukken:

$$\chi^\nu = \mathrm{R}(\Phi, c_1, \ldots c_m).$$

De functie χ, die bij de alleenstaande ondergroep g van ondeelbaren aanwijzer behoort, is dus uit eene binomische vergelijking van ondeelbaren graad te bepalen.

§ 67. Het algemeene plan voor de oplossing eener hoogere-machtsvergelijking, in § 64 geschetst, moet nu in zooverre nader gepreciseerd worden, dat men niet geheel vrij is in de keuze van eene ondergroep g in de groep G: neemt men voor g eene alleenstaande ondergroep van ondeelbaren aanwijzer in G, voor g′ eene

alleenstaande ondergroep van priem index in g, enz., dan worden alle resolventen, die ons achtereenvolgens de functiën φ, φ', ... doen vinden, binomische vergelijkingen.

We worden er dus nu toe geleid, te onderzoeken of het mogelijk is uit de symmetrische groep af te zonderen eene alleenstaande ondergroep van priem index; uit deze weer eene in deze groep alleenstaande ondergroep van priem index, enz totdat wij eindelijk komen tot de groep 1.

HOOFDSTUK IV.

ONTBINDING VAN GROEPEN.

§ 68. Elke groep G bevat als alleenstaande ondergroepen zich zelve en de identische groep. Bevat G geen andere alleenstaande ondergroep, dan heet G enkelvoudig; in het tegengestelde geval heet G samengesteld.

Voorbeelden. 1. Eene cyclische groep van ondeelbaren graad b.v. $s_1, s_1^2, s_1^3, s_1^4, s_1^5, s_1^6 = 1$ bevat geen enkele ondergroep, dus ook geen alleenstaande ondergroep. De groep is dus enkelvoudig.

2. Eene cyclische groep van deelbaren graad, b.v. $s_1, s_1^2, s_1^3, s_1^4, s_1^5, s_1^6 = 1$ bevat als ondergroep de groep $s_1^2, s_1^4, s_1^6 = 1$ en dit is eene alleenstaande ondergroep (§ 50, voorbeeld 2). De groep is dus samengesteld.

§ 69. Is de groep G samengesteld, dan kan men uit G eene alleenstaande ondergroep g afzonderen; is g weer samengesteld, dan kan men in g eene alleenstaande ondergroep g′ vinden; zoo voortgaande moet men eindelijk tot eene enkelvoudige groep komen, waarin 1 de eenige alleenstaande groep is. De reeks G, g, g′, g″, ... 1 heet *de samenstellende reeks* van de groep G, als men er ten minste voor gezorgd heeft, dat de groep g de grootste in G aanwezige alleenstaande groep is, dat m. a. w. er niet eene groep bestaat, die alleenstaande in G is en g bevat; en als hetzelfde geldt voor g′ in g enz.

De groepen g′, g″,... behoeven niet in G alleenstaande te zijn.

Is de index van g in G 't getal ν, van g′ in g 't getal ν',... enz., eindelijk van 1 in de voorafgaande groep $\nu^{(i)}$, dan heeten $\nu, \nu', \dots \nu^{(i)}$ de *samenstellingsfactoren* van G.

Voorbeeld. De groep $s, s^2, \dots s^{12} = s_0 = 1$ bevat de maximale alleenstaande ondergroep $s^2, s^4, s^6, s^8, s^{10}, 1$ van den index 2. Deze groep bevat de maximale alleenstaande ondergroep $s^4, s^8, 1$ van den index 2, terwijl de ondergroep 1 in deze enkelvoudige groep den index 3 heeft. De samenstellingsfactoren zijn dus hier 2, 2, 3.

§ 70. Het is soms mogelijk verschillende samenstellende reeksen voor eene zelfde groep op te schrijven. De cyclische groep van de 12de orde is b.v. ook te ontbinden in $g = (s^3, s^6, s^9, s^{12} = 1)$; $g' = (s^6, s^{12} = 1)$; $g'' = 1$. De samenstellingsfactoren zijn in dit geval 3, 2, 2.

JORDAN [1]) heeft bewezen, dat de samenstellingsfactoren eener zelfde groep bij verschillende ontbindingen alleen in volgorde kunnen verschillen. De samenstellingsfactoren eener cyclische groep zijn altijd, in de eene of andere volgorde, de priemfactoren van haar orde.

§ 71. De alterneerende groep G van meer dan vier letters is enkelvoudig [2]).

Bewijs. Eene alleenstaande ondergroep g van G zou geen cyclische substitutie van drie letters $(x_0\, x_1\, x_2)$ kunnen bevatten, want was dat het geval dan zou men deze kunnen transformeeren door de substitutie

$$\begin{pmatrix} x_0\, x_1\, x_2\, x_3\, x_4\, \dots \\ x_\alpha\, x_\beta\, x_\gamma\, x_\delta\, x_\varepsilon\, \dots \end{pmatrix} \text{ of } \begin{pmatrix} x_0\, x_1\, x_2\, x_3\, x_4\, \dots \\ x_\alpha\, x_\beta\, x_\gamma\, x_\varepsilon\, x_\delta\, \dots \end{pmatrix}$$

waarvan er ééne zeker tot G behoort; uit $(x_0\, x_1\, x_2)$ zou men dan vinden $(x_\alpha\, x_\beta\, x_\gamma)$ en deze zou zeker tot de

1) JORDAN, bldz 42. HÖLDER, Math. Ann. XXXIV. PIERPONT, Am. Journ. of Math. XVIII.

2) JORDAN, bldz. 63; WEBER, I § 177.

alleenstaande ondergroep behooren. Maar zoo zou men dit van elke cyclische substitutie van drie letters kunnen bewijzen en dan zou de groep, blijkens hetgeen in het 2de voorbeeld van § 39 gezegd is, de alterneerende groep moeten bevatten. De groep g kan dus geen cyclische substitutie van drie letters bevatten zonder met G samen te vallen.

Het zal nu blijken, dat welke substitutie s men ook onderstelt tot g te behooren, daaruit afgeleid kan worden, dat g eene cyclische substitutie van drie letters bevat en dus met G samenvalt. Te gelijk met s is ook, als σ eene substitutie van G is, $\sigma^{-1} s \sigma$ eene substitutie van g en $s^{-1} \sigma^{-1} s \sigma$ insgelijks. Deze substitutie nu zal, als men σ eenvoudig kiest, veel eenvoudiger dan s worden, omdat alle letters, die door σ niet omgezet worden, door deze substitutie niet verplaatst zullen worden: want zij worden achtereenvolgens alleen verplaatst door s^{-1} en s. Gaan we nu alle mogelijke onderstellingen voor s na.

1°. Laat s een cyclus van meer dan 3 letters bevatten: $s = (x_0 x_1 x_2 x_3 \dots x_k) \dots$. Neem dan $\sigma = (x_0 x_1 x_2)$ dan wordt $s^{-1} \sigma^{-1} s \sigma = (x_0 x_k \dots x_3 x_2 x_1)(x_1 x_2 x_0 x_3 \dots x_k) = (x_0 x_1 x_3)$. g wordt dan tot G.

2°. Laat s twee cycli van drie letters bevatten: $s = (x_0 x_1 x_2)(x_3 x_4 x_5)$.

Neemt men dan $\sigma = (x_0 x_2 x_3)$ dan wordt $s^{-1} \sigma^{-1} s \sigma = (x_0 x_2 x_1)(x_3 x_5 x_4)(x_2 x_1 x_3)(x_0 x_4 x_5) = (x_0 x_1 x_4 x_2 x_3)$, maar deze substitutie zou weer leiden tot eene cyclische substitutie van drie letters.

3°. Laat nu $s = (x_0 x_1 x_2)(x_3 x_4) \dots$ [1]); kiest men dan $\sigma = (x_0 x_1 x_3)$ dan wordt $s^{-1} \sigma^{-1} s \sigma = (x_0 x_2 x_1)(x_3 x_4)(x_1 x_3 x_2)(x_0 x_4) = (x_0 x_1 x_4 x_2 x_3)$.

4°. Bevat s drie transposities $s = (x_0 x_1)(x_2 x_3)(x_4 x_5) \dots$

---

[1]) Daar 't aantal transposities even moet zijn, moet hier nog iets volgen.

dan vindt men voor $\sigma = (x_0 x_2 x_4)$ $s^{-1}\sigma^{-1}s\sigma = (x_0 x_1)(x_2 x_3)(x_4 x_5)(x_2 x_1)(x_4 x_3)(x_0 x_5) = (x_0 x_2 x_4)(x_1 x_5 x_3)$ en dit gaat niet blijkens 2°.

5°. Bevat eindelijk s twee transposities en één element, dat niet verplaatst wordt: $s = (x_0 x_1)(x_2 x_3)(x_4)$, dan vindt men als $\sigma = (x_0 x_1 x_4)$ is: $s^{-1}\sigma^{-1}s\sigma = (x_0 x_1)(x_2 x_3)(x_1 x_4)(x_2 x_3) = (x_0 x_4 x_1)$; ook dit kan dus niet. Hiermede zijn alle gevallen behandeld: de alterneerende groep van meer dan 4 letters is dus enkelvoudig.

Is het aantal letters 4, dan kan men voor s ook nog het geval nemen, dat zij uit twee transposities bestaat en dan vindt men juist de alleenstaande ondergroep

$$1 \quad (x_0 x_1)(x_2 x_3) \quad (x_0 x_2)(x_1 x_3) \quad (x_0 x_3)(x_1 x_2),$$

de viergroep, waarop reeds in § 51 is gewezen.

§ 72. Komen we nu nog eens terug op de algebraïsche oplosbaarheid der algemeene hoogere-machtsvergelijkingen, dan kunnen we den eisch voor de oplosbaarheid, in § 67 gegeven, nu aldus formuleeren: de samenstellingsfactoren der groep moeten priemgetallen zijn.

§ 73. De symmetrische groep van drie letters

$$1 \quad (x_1 x_2) \quad (x_0 x_1 x_2) \quad (x_0 x_1) \quad (x_0 x_2 x_1) \quad (x_0 x_2)$$

heeft tot samenstellende reeks de alterneerende groep 1, $(x_0 x_1 x_2)$, $(x_0 x_2 x_1)$ en de identische groep, waarvan de factoren zijn 2, 3 De algemeene derdemachtsvergelijking is dus algebraïsch op te lossen.

De symmetrische groep G van vier letters heeft tot samenstellende reeks: de groep G, de alterneerende groep, de viergroep, de groep *1*, $(x_0 x_1)(x_2 x_3)$, de identiteit. De samenstellingsfactoren zijn dus 2, 3, 2, 2. Dit zijn priemgetallen: de vierdemachtsvergelijking is dus algebraïsch op te lossen.

De symmetrische groep G van meer dan 4 letters bestaat uit G, de alterneerende groep en vervolgens, daar de alterneerende groep enkelvoudig is, de identische

groep. De samenstellingsfactoren zijn dus $2, \frac{m!}{2}$. Deze getallen zijn niet priem: de algemeene m^{de}-machtsvergelijking is dus voor $m > 4$ niet algebraïsch op te lossen op de wijze, waartoe wij hier gekomen zijn.

§ 74. Het zou ondertusschen de vraag zijn of men niet tot eene oplossing zou kunnen komen, wanneer men zich niet, zooals wij gedaan hebben, beperkte tot het beschouwen van geheele, rationale functiën der wortels. Maar in plaats van deze lacune aan te vullen, stappen we liever af van de beschouwing van de zeer speciale vergelijkingen, die we tot nu toe behandeld hebben, om het vraagstuk in zijne volle algemeenheid onder handen te nemen.

De vergelijkingen met geheel onbepaalde lettercoëfficienten vormen n.l. niet het algemeenste geval: zijn de wortels onafhankelijk veranderlijke grootheden, dan zijn functiën dier wortels alleen dan gelijk als zij identiek zijn. Heeft men daarentegen te doen met vergelijkingen met getallen-coëfficienten, dan kunnen functiën der wortels wel degelijk gelijk zijn zonder identiek te wezen. En deze numerieke gelijkheid kunnen we niet voorbijzien. Want de stelling, dat de substituties, die eene rationale functie der wortels onveranderd laten, eene groep vormen, blijft niet waar, wanneer slechts geëischt wordt dat zij numeriek onveranderd blijft. Was toch φ eene functie, die door de substituties s_1 en s_2 niet veranderd werd, dan konden we vroeger zeggen: pas op $\varphi = \varphi_{s_1}$ de substitutie s_2 toe, dan komt er $\varphi_{s_2} = \varphi_{s_1 s_2}$, maar daar $\varphi_{s_2} = \varphi$ is, is ook $\varphi_{s_1 s_2} = \varphi$ en blijft dus φ door het product der substituties s_1 en s_2 ook onveranderd. Deze redeneering was juist zoolang φ en φ_{s_1} identiek waren: zijn ze enkel numeriek gelijk, dan behoeven φ en φ_{s_1} volstrekt niet hetzelfde op te leveren als zij aan eene zelfde substitutie worden onderworpen.

Voorbeeld. De vergelijking

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

heeft tot wortels

$$x_0 = \epsilon \,,\quad x_1 = \epsilon^2,\quad x_2 = \epsilon^3$$
$$x_3 = \epsilon^4,\quad x_4 = \epsilon^5,\quad x_5 = \epsilon^6$$

als ϵ eene complexe 7de-machtswortel der eenheid is. De functiën der wortels

$$x_1 x_5^4,\quad x_2 x_3^4,\quad x_3 x_1^4,\quad x_5 x_4^4$$

hebben alle dezelfde waarde ϵ^5 en voor geen andere waarden van i en j krijgt $x_i x_j^4$ dezelfde waarde ϵ^5. Dat de substituties, die $x_1 x_5^4$ in deze 4 waarden overvoeren, n.l.

$$1,\quad (x_1 x_2)(x_3 x_5),\quad (x_1 x_3 x_5),\quad (x_1 x_5 x_4)$$

geen groep vormen, is zonder nader onderzoek duidelijk, omdat de 2de-machten der laatste twee substituties er niet bij zijn.

De substituties, die eene functie van de wortels numeriek onveranderd laten, behoeven dus volstrekt geen groep te vormen. Daarmee is de grondslag verdwenen, waarop de geheele theorie omtrent het verband tusschen rationale functiën en substitutiegroepen was opgetrokken. Schijnt daarmee deze theorie geheel te vallen, bij nader inzien zal blijken, dat er heel wat van te redden is: het komt er maar op aan, de beschouwingen, waarbij het de vraag was, welke functiën van m onafhankelijk veranderlijken door algebraïsche bewerkingen uit de symmetrische functiën dier veranderlijken konden worden opgebouwd, uit te breiden tot het geval, dat de onafhankelijk veranderlijken bekende grootheden worden.

Daarvoor is het echter noodig van naderbij te beschouwen de verzamelingen van getallen, die ontstaan als op een stel gegeven grootheden op alle mogelijke wijzen de vier hoofdbewerkingen der algebra worden uitgevoerd.

HOOFDSTUK V.

GETALLENLICHAMEN, ALGEBRAÏSCHE LICHAMEN. LICHAAM VAN GALOIS EENER VERGELIJKING.

§ 75. Onder een *getallenlichaam* verstaat men eene verzameling van getallen van dien aard, dat door optelling, aftrekking, vermenigvuldiging en deeling van deze getallen geen andere getallen ontstaan dan die tot de verzameling behooren. Deeling door nul, eene onmogelijke bewerking, wordt hierbij uitgesloten.

Het begrip getallenlichaam, zij het dan ook in zeer elementairen vorm, vindt men het eerst bij GALOIS. [1]) DEDEKIND [2]) heeft de getallenlichamen, het eerst uitvoerig behandeld.

Daar de eenheid ontstaat door de deeling van twee gelijke getallen, bevat elk getallenlichaam de eenheid en daarmee alle geheele en gebroken getallen.

De verzameling der rationale getallen is dus het eenvoudigste lichaam, wanneer men ten minste het lichaam, door het getal nul alleen gevormd, buiten beschouwing laat.

---

[1]) GALOIS, Oeuvres, bldz. 35.

[2]) DIRICHLET-DEDEKIND Zahlentheorie § 159 in den 2den druk (1871) en de volgende drukken; DEDEKIND in *Bull. de Darboux*, I, 1877. KRONECKER. *Grundzüge einer arithm Theorie der algebr. Grössen. Crelle's Journal*, Bnd. 92. KRONECKER (en anderen) spreekt van een Rationalitätsbereich. Vergelijk voor dit geheele hoofdstuk: WEBER, Algebra I, Buch III.

Alle reëele getallen vormen ook een lichaam.

Evenzoo alle complexe getallen (met de reëele getallen er bij).

§ 76. Men kan de getallen van een lichaam Ω door de vier hoofdbewerkingen verbinden met het getal x, dat niet in het lichaam Ω voorkomt. Daardoor ontstaan nieuwe getallen, die met de oude een nieuw lichaam Ω' vormen. Men zegt dan, dat het lichaam Ω' uit Ω door toevoeging van x is ontstaan.

Men kan ook meer grootheden of een lichaam aan een lichaam toevoegen.

Het lichaam der complexe getallen ontstaat b.v. door toevoeging van $\sqrt{-1}$ aan dat der reëele getallen.

§ 77. Eene geheele rationale functie van x,

$$f(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_n$$

welker coefficienten tot het lichaam Ω behooren, heet eene functie in Ω. Zulk eene functie kan in Ω ontbindbaar of niet-ontbindbaar zijn. De ontbindbaarheid hangt werkelijk samen met de uitgebreidheid van Ω [1]); de functie

$$\begin{aligned} x^4 + 100 &= (x^2 - 2x\sqrt{5} + 10)(x^2 + 2x\sqrt{5} + 10) \\ &= (x - \sqrt{5} - \sqrt{-5})(x - \sqrt{5} + \sqrt{-5}) \\ &\qquad (x + \sqrt{5} - \sqrt{-5})(x + \sqrt{5} + \sqrt{-5}) \end{aligned}$$

is onontbindbaar in het lichaam der rationale getallen, ontbindbaar in 2 tweedegraadsfactoren, als men $\sqrt{5}$ aan 't lichaam der rationale getallen toevoegt en in 4 eerstegraadsfactoren, als men daarna $\sqrt{-1}$ toevoegt.

Elke functie wordt ontbindbaar, als een harer wortels aan het lichaam wordt toegevoegd.

§ 78. Heeft eene functie $F(x)$ in Ω éen wortel van eene in dezen zin onontbindbare functie $f(x)$ in Ω, dan heeft zij alle wortels van $f(x)$. Want de grootste gemeene

---

[1]) GALOIS, Oeuvres, bldz. 35.

deeler van $F(x)$ en $f(x)$, die door rationale bewerkingen te vinden is, is eene functie in Ω. Maar $f(x)$ heeft geen andere deelers in Ω dan zich zelf of een getal van Ω.

§ 79. Is $F(x)$ eene functie in Ω, die geen twee gelijke wortels heeft, dan ontstaat door toevoeging van een wortel a van $F(x)$ aan 't lichaam een nieuw getallenlichaam $\Omega(a)$ dat we een *algebraïsch lichaam* noemen.

Is $F(x)$ ontbindbaar en is

$$f(x) = x^n + c_1 x^{n-1} + \ldots c_n \tag{1}$$

de onontbindbare factor van $F(x)$, die den wortel a bevat, dan heet het lichaam $\Omega(a)$ van den n^{den} graad.

§ 80. Elke grootheid in het algebraïsch lichaam $\Omega(a)$ kan als eene geheele rationale functie van a, of korter, als eene functie van a in Ω, van lageren dan den n^{den} graad geschreven worden.

Bewijs. Door elementaire herleidingen is elk algebraïsch getal, dat door optelling, aftrekking, vermenigvuldiging en deeling van a en de getallen van Ω kan ontstaan, te brengen tot den vorm $\frac{\varphi(a)}{\psi(a)}$, als φ en ψ functien in Ω zijn, die geen factor gemeen hebben. Men kan den teller nu zoo schrijven, dat de deeling opgaat.

$\psi(x)$ toch zal onderling ondeelbaar moeten zijn met $f(x)$, daar anders de noemer nul zou worden. Bij twee onderling ondeelbare geheele functiën $\psi(x)$ en $f(x)$ kan men echter altijd 2 zulke geheele functiën $g_1(x)$ en $g_2(x)$ bepalen, dat identiek:

$$\psi(x)\, g_1(x) + f(x)\, g_2(x) = 1 \quad [1]$$

---

[1]) Zoekt men n.l. den g. g. d. van $\psi(x)$ en $f(x)$ door deeling, noemt men 't 1ste quotient Q_1, de 1ste rest R_1, 't 2de quotient Q_2, de 2de rest R_2, enz., dan is

$$\begin{aligned} R_1 &= f(x) - Q_1 \,.\, \psi(x) \\ R_2 &= \psi(x) - Q_2\, R_1 \\ R_3 &= R_1 - Q_3 \,.\, R_2 \\ &\ldots\ldots\ldots \\ R_n &= R_{n-2} - Q_n \,.\, R_{n-1} \end{aligned}$$

De breuk $\frac{\varphi(x)}{\psi(x)}$ kan dus ook geschreven worden:

$$\frac{\varphi(x)\{\psi(x)g_1(x)+f(x)g_2(x)\}}{\psi(x)}$$

en nu wordt, als men $x=a$ stelt:

$$\frac{\varphi(a)}{\psi(a)}=\varphi(a)g_1(a)=\chi(a).$$

Is bij de deeling van $\chi(x)$ door $f(x)$ het quotient $q(x)$ en de rest $r(x)$, dan is deze rest van lageren dan den n^{den} graad. $x=a$ stellende vindt men nu

$$\frac{\varphi(a)}{\psi(a)}=r(a).$$

Voorbeeld. Elke grootheid in 't lichaam $\Omega(i)$, waarbij i een wortel is van de vergelijking $x^2+1=0$ kan uitgedrukt worden als eene geheele rationale functie van i van lageren dan den 2^{den} graad.

§ 81. Elke grootheid in $\Omega(a)$ kan ook maar op éene wijze zoo uitgedrukt worden, want de gelijkstelling van twee dergelijke uitdrukkingen zou eene vergelijking geven van lageren dan den n^{den} graad, die met de onontbindbare vergelijking van den n^{den} graad $f(x)=0$ een wortel a gemeen zou hebben.

§ 82. Zijn $a_1, a_2, \ldots a_{n-1}$ de andere wortels van de vergelijking (1), dan kan men ook vormen de lichamen

$$\Omega(a_1),\ \Omega(a_2), \ldots\ \Omega(a_{n-1})$$

die de *toegevoegde lichamen* van $\Omega(a)$ heeten.

De laatste rest is geen functie van x. Drukt men nu met behulp van deze betrekkingen achtereenvolgens de resten $R_2, \ldots R_n$ uit in $f(x)$, $\psi(x)$ en de Q's, dan vindt men ten slotte

$$R_n = P_1(x)\,\psi(x) + P_2(x)\,f(x)$$

waarin P_1 en P_2 geheele functiën der Q's en dus van x blijken te zijn. Deelt men door 't getal R_n, dan vindt men de toegepaste stelling. (Zie WEBER, Algebra I, § 6).

§ 83. Is $\alpha = r(a)$ eene grootheid in $\Omega(a)$, dus eene geheele, rationale functie van a van lageren dan den n^{den} graad met coëfficienten, die tot Ω behooren, dan kan men vormen de grootheden

$$\alpha_1 = r(a_1),\ \alpha_2 = r(a_2) \ldots .\ \alpha_{n-1} = r(a_{n-1}).$$

Deze grootheden heeten de *toegevoegden* van $r(a)$.

Onder de toegevoegde grootheden kunnen gelijke voorkomen. Het is echter gemakkelijk toegevoegde grootheden te vinden, die alle verschillen. Daartoe behoeft men slechts de k's in

$$r(a) = k_1 a^{n-1} + k_2 a^{n-2} + \ldots\ldots + k_n$$

zóó te kiezen, dat niet voldaan wordt aan eenige vergelijking

$$r(a_i) = r(a_j)$$

hetgeen altijd mogelijk is omdat er volgens onderstelling onder de a's geen gelijke voorkomen.

§ 84. Onderstellen we dus $\alpha, \alpha_1, \ldots .\ \alpha_{n-1}$ verschillend. Deze grootheden zijn de wortels eener n^{de} machtsvergelijking

$$\Phi(\xi) \equiv (\xi - \alpha)(\xi - \alpha_1) \ldots\ldots (\xi - \alpha_{n-1}) = 0.$$

De coëfficienten zijn symmetrische functiën der wortels $\alpha, \alpha_1, \ldots\ldots \alpha_{n-1}$: zij kunnen dus rationaal in de coëfficienten der vergelijking (1) § 79 uitgedrukt worden en zijn dus grootheden in Ω.

Laat $\varphi(\xi)$ een onontbindbare factor zijn van $\Phi(\xi)$, dan moet $\varphi(\xi)$ zeker voor ééne der waarden α nul worden. Is nu

$$\varphi(\alpha) = \varphi[r(a)] = 0,$$

dan hebben de vergelijkingen

$$\varphi[r(x)] = 0 \text{ en } f(x) = 0$$

een wortel a gemeen. De laatste vergelijking is onont-

bindbaar: alle wortels van $f(x) = 0$ voldoen dus aan de eerste vergelijking. Derhalve is

$$\varphi[r(a_1)] = 0,\ \varphi[r(a_2)] = 0, \ldots\ \varphi[r(a_{n-1})] = 0$$

of

$$\varphi(\alpha_1) = 0,\ \varphi(\alpha_2) = 0, \ldots\ \varphi(\alpha_{n-1}) = 0$$

$\varphi(\xi)$ wordt dus nul voor de n verschillende waarden $\alpha, \alpha_1, \alpha_2, \ldots \alpha_{n-1}$, $\varphi(\xi)$ verschilt dus niet van $\Phi(\xi)$, derhalve is $\Phi(\xi)$ in dit geval onontbindbaar.

§ 85. Zijn de toegevoegde grootheden $\alpha, \alpha_1, \ldots \alpha_{n-1}$ niet alle verschillend, maar komen er slechts p verschillende onder voor, dan zal $\varphi(\xi)$ slechts voor al deze p waarden nul worden en elke andere onontbindbare factor van $\Phi(\xi)$ zal dezelfde wortels hebben. $\Phi(\xi)$ zal dus eene macht van $\varphi(\xi)$ moeten zijn en p zal een factor van n wezen.

In deze en de vorige § is dus bewezen:
elke grootheid α van een algebraïsch lichaam $\Omega(a)$ van den n^{den} graad is te vinden uit eene n^{de}-machtsvergelijking in Ω; die vergelijking is onontbindbaar als α en al hare toegevoegde grootheden verschillen. Zijn er maar p ongelijke onder, dan moet p een factor van n zijn en is de vergelijking de $(n:p)^{de}$-macht van eene onontbindbare vergelijking van den p^{den} graad.

Voorbeeld. Elke complexe grootheid is de wortel van eene reëele vierkantsvergelijking, die onontbindbaar is; de andere wortel is de toegevoegde complexe grootheid.

§ 86. Als de grootheden $\alpha, \alpha_1, \ldots \alpha_{n-1}$ alle onderling verschillen, heet $\alpha = r(a)$ eene *primitieve grootheid* in het lichaam $\Omega(a)$.

Zijn er, behalve de getallen van Ω, geen andere imprimitieve grootheden in $\Omega(a)$, dan heet $\Omega(a)$ een *primitief lichaam*.

§ 87. De primitieve grootheden spelen een belangrijke rol in een algebraïsch lichaam: elke grootheid van het

lichaam $\Omega(a)$ kan n.l. rationaal in eene willekeurige primitieve grootheid van het lichaam $\Omega(a)$ uitgedrukt worden. Is toch ω eene grootheid van $\Omega(a)$ en zijn ω_1, $\omega_2, \ldots \omega_{n-1}$ de toegevoegde grootheden; zijn $\alpha, \alpha_1, \ldots$ α_{n-1} toegevoegde primitieve grootheden en is

$$\Phi(\xi) = (\xi - \alpha)(\xi - \alpha_1) \ldots (\xi - \alpha_{n-1})$$

dan stelt

$$\Phi(\xi) \left\{ \frac{\omega}{\xi - \alpha} + \frac{\omega_1}{\xi - \alpha_1} + \ldots + \frac{\omega_{n-1}}{\xi - \alpha_{n-1}} \right\}$$

eene geheele functie van den $n - 1^{sten}$ graad in ξ voor, welker coëfficienten symmetrische functiën van de wortels $a, a_1, \ldots a_{n-1}$ zijn: het is dus eene functie in Ω Noemen we deze functie $\Psi(\xi)$, dan vinden we, als we $\xi = \alpha$ stellen:

$$\omega = \frac{\Psi(\alpha)}{\Phi'(\alpha)},$$

ω is dus rationaal in α uit te drukken. Hieruit volgt, dat het lichaam $\Omega(a)$ even goed kan genoemd worden een lichaam $\Omega(\alpha)$: men kan het ook beschouwen als ontstaan te zijn door toevoeging aan Ω van een wortel α der onontbindbare vergelijking in Ω $\Phi(\xi) = 0$.

§ 88. Daar de grootheden $a, a_1, \ldots a_{n-1}$ als wortels van eene onontbindbare vergelijking in een eigenaardig verband tot elkaar staan, is het niet te verwonderen, dat de lichamen $\Omega(a), \Omega(a_1), \ldots \Omega(a_{n-1})$ niet altijd onafhankelijk van elkaar zijn. Het kan zelfs gebeuren, dat deze lichamen identiek zijn. In dit geval heet het lichaam een *lichaam van Galois* of een *normaal lichaam*.

In dit geval behooren $a_1, \ldots a_{n-1}$ tot $\Omega(a)$ en zijn dus alle wortels van (1) rationaal in a uit te drukken. Maar daar elk der lichamen $\Omega(a_i)$ dan een normaal lichaam is, kunnen de wortels der vergelijking (1) rationaal in *elk* hunner worden uitgedrukt.

Ook de toegevoegde grootheden van een primitief element kunnen in dit geval rationaal in dit element uitgedrukt worden.

§ 89. Voegt men alle wortels van eene vergelijking van den m^{den} graad

$$F(x) = 0 \qquad (2)$$

aan het lichaam Ω toe, dan krijgt men een lichaam, dat men kan voorstellen door $\Omega(a, a_1, \ldots\ldots a_{m-1})$. Dit lichaam kan ook verkregen worden door één wortel eener andere vergelijking aan Ω toe te voegen. Neem toch de functie der wortels:

$$V = \lambda a + \lambda_1 a_1 + \lambda_2 a_2 + \ldots \lambda_{m-1} a_{m-1}.$$

Onderstellen we, dat door alle substituties $s, s_1\, s_2, \ldots s_{m!-1}$ van de wortels deze functie overgaat in $V, V_1, V_2, \ldots V_{m!-1}$ en dat de grootheden $\lambda, \lambda_1, \ldots \lambda_{m-1}$ zoo gekozen zijn dat geen twee waarden V_i gelijk zijn, dan is de functie

$$\Phi(\xi) = (\xi - V)(\xi - V_1) \ldots (\xi - V_{m!-1})$$

eene functie van ξ in Ω. Is nu ω eene grootheid van het lichaam $\Omega(a, a_1, \ldots\ldots a_{m-1})$ en dus eene geheele rationale functie van $a, a_1, \ldots a_{m-1}$; zijn $\omega_1, \omega_2, \ldots \ldots \omega_{m!-1}$ de waarden, waarin ω overgaat door de substituties $s, s_1, \ldots s_{m!-1}$, dan is

$$\Phi(\xi)\left\{\frac{\omega}{\xi - V} + \frac{\omega_1}{\xi - V_1} + \ldots \frac{\omega_{m!-1}}{\xi - V_{m!-1}}\right\} = \Psi(\xi)$$

eene functie van ξ van den graad $m! - 1$. Voor $\xi = V$ vindt men hieruit

$$\omega = \frac{\Psi(V)}{\Phi'(V)} = \chi(V).$$

Evenzoo vindt men door $\xi = V_i$ te stellen:

$$\omega_i = \frac{\Psi(V_i)}{\Phi'(V_i)} = \chi(V_i).$$

ω is dus eene grootheid van $\Omega(V)$, het algebraïsch lichaam,

dat ontstaat als men aan Ω toevoegt den wortel V van een onontbindbaren factor der vergelijking $\Phi(\xi) = 0$.

Daar ook elke grootheid van $\Omega(V)$ voorkomt in het lichaam $\Omega(a, a_1, \ldots . a_{m-1})$, zijn de lichamen Ω (V) en $\Omega(a, a_1, \ldots . a_{m-1})$ identiek.

§ 90. Het lichaam $\Omega(V)$ is een normaal lichaam, want is de onontbindbare factor van de vergelijking $\Phi(\xi) = 0$ waaraan V voldoet

$$\varphi(\xi) \equiv (\xi - V)(\xi - V_1) \ldots . (\xi - V_{n-1}) = 0 \qquad (3)$$

dan zijn blijkens het voorgaande $V_1, V_2, \ldots . V_{n-1}$ ook grootheden van het lichaam $\Omega(a, a_1, \ldots . a_{m-1})$ en dus van het lichaam $\Omega(V)$.

De vergelijking (3) heet de *resolvente van* Galois van de gegeven vergelijking (2) in § 89. De graad er van is blijkbaar een deeler van $m!$ Kan deze resolvente opgelost worden, dan vindt men V en daardoor alle grootheden van het lichaam $\Omega(V)$, dus ook de wortels $a, a_1, \ldots . a_{m-1}$ der gegeven vergelijking. Oorspronkelijk zijn natuurlijk alleen de grootheden van het lichaam Ω, dat uit de coëfficienten der vergelijking (2) wordt afgeleid, bekend.

§ 91. Daar het lichaam $\Omega(V)$ een normaal lichaam is, kunnen de grootheden $V_1, V_2, \ldots . V_{n-1}$ als geheele rationale functiën van V van hoogstens den graad $n-1$ geschreven worden met coëfficienten uit Ω. Wij stellen dus:

$$V_1 = r_1(V),\ V_2 = r_2(V),\ \ldots .\ V_{n-1} = r_{n-1}(V).$$

Substitueert men in eene functie in Ω van V de aan V toegevoegde wortels, dan ontstaan de toegevoegde functiën, die met de gegeven functie, wortels zijn van eene onontbindbare n^{de}-machtsvergelijking in Ω.

Past men dit toe op $r_i(V)$, dan zijn dus

$$r_i(V),\ r_i(V_1),\ r_i(V_2) \ldots .\ r_i(V_{n-1})$$

de wortels eener onontbindbare n^{de}-machtsvergelijking; deze vergelijking heeft met de onontbindbare Galois'sche

resolvente (3) een wortel $r_i(V) = V_i$ gemeen, alle wortels zijn dus aan beide vergelijkingen gemeenschappelijk.

De grootheden

$$r_i(V),\ r_i(V_1),\ r_i(V_2) \ldots\ r_i(V_{n-1})$$

blijken dus de wortels $V, V_1, V_2, \ldots V_{n-1}$ in andere volgorde te zijn.

De grootheid $r_i(V_k)$ wordt verkregen door eerst op V de substitutie s_i toe te passen: men vindt dan V_i of $r_i(V)$; daarna vervangt men V door V_k, d. w. z. men past daarna de substitutie s_k toe. Het blijkt dus, dat als twee substituties s_i en s_k uit V eene der toegevoegde grootheden $V, V_1, V_2, \ldots V_{n-1}$ doen ontstaan, het product dier substituties ook uit V eene dier toegevoegde grootheden doet ontstaan en dus tot de verzameling der substituties behoort:

> de substituties $s, s_1, s_2, \ldots s_{n-1}$, die eene primitieve grootheid V van het lichaam van GALOIS der vergelijking $F(x) = 0$ in de toegevoegde grootheden overvoeren, vormen eene groep G.

Deze groep heet de *groep van* GALOIS *van het lichaam* $\Omega(V)$ of ook de *groep van* GALOIS *van de vergelijking* $F(x) = 0$.

§ 92. De groep van GALOIS bezit de volgende twee fundamenteele eigenschappen:

I. Elke functie in Ω van de wortels van $F(x) = 0$ die een getal van 't lichaam Ω is, blijft onveranderd door de substituties van G.

II. Elke functie in Ω van de wortels van $F(x) = 0$, die (numeriek) onveranderd blijft door alle substituties van G, is een getal van Ω [1]).

Bewijs. I. Is ω eene functie in Ω van de wortels $a, a_1, \ldots a_{m-1}$, dan kan men de wortels in V uitdrukken en zoo in overeenstemming met § 89 vinden $\omega = \chi(V)$.

---

[1]) GALOIS. Oeuvres, p. 38 Proposition I.

Voert men eerst op de wortels de substitutie s_i der Galois'sche groep uit, dan krijgt men ω_i, die volgens § 89 dezelfde functie χ van V_i is: $\omega_i = \chi\,(V_i)$. Is echter $\chi(V) = C$ of V een wortel van $\chi(\xi) - C = 0$, dan zijn ook $V_1, V_2, \ldots V_{n-1}$ wortels dezer vergelijking, derhalve is

$$\chi(V_1) = \chi(V_2) = \ldots = \chi(V_{n-1}) = C.$$

II. Blijft eene functie in Ω van $a, a_1, \ldots a_{m-1}$ numeriek onveranderd door alle substituties van G, dan is die functie gelijk aan $\frac{1}{n}(\chi + \chi_1 + \chi_2 + \ldots + \chi_{n-1})$ d.i. eene symmetrische functie der grootheden V, die dus uit te drukken is in de coëfficienten van $\varphi(\xi)$ d.i. in getallen van 't lichaam Ω

Uit I volgt nog, dat elke rationale betrekking in Ω tusschen de wortels van $F(x) = 0$ waar blijft, als men er eene substitutie van G op toepast.

§ 93. Gelden omgekeerd deze twee eigenschappen voor eenige substitutiegroep, dan is die groep de groep van Galois der vergelijking.

Bewijs. Blijft elke rationale betrekking in Ω tusschen de wortels waar, als men er eene substitutie s_i op toepast; is de resolvente van Galois $\varphi(\xi) = 0$, en voldoet hieraan de functie V van de wortels $a, a_1, \ldots a_{m-1}$, dus is $\varphi\,(V) = 0$; dan blijft deze rationale betrekking waar, als men er de substitutie s_i op toepast, waardoor V in V_i overgaat. Derhalve is $\varphi(V_i)$ ook nul, maar dan is V_i een wortel van de Galois'sche resolvente en s_i eene substitutie van de groep van Galois. Bezit dus eene groep G′ de eigenschap, dat elke in Ω rationale betrekking tusschen de wortels waar blijft, als men er haar substituties op toepast, dan is G′ de groep G zelf of een harer ondergroepen.

Bezit eene groep $G' = (s, s_\alpha, s_\beta, \ldots)$ de eigenschap, dat elke in Ω rationale functie van de wortels $a, a_1, \ldots a_m$,

die (numeriek) onveranderd blijft door de substituties van G′, een getal van Ω is, dan is

$$(\xi - V)(\xi - V_\alpha)(\xi - V_\beta)\ldots.$$

eene functie van ξ, met coëfficienten, die onveranderd blijven door de substituties van G′; volgens het onderstelde zijn de coëfficienten dus getallen van Ω. Maar dan moet de resolvente van Galois, die onontbindbaar is en den factor $\xi - V$ bevat, een deeler hiervan zijn. De groep van Galois is dus de groep G′ zelf of een ondergroep er van.

Volgens het eerste deel van 't bewijs is dus G′ de groep G of een van hare ondergroepen; volgens het tweede deel is G′ de groep G of is G een ondergroep van G′. Derhalve moet G′ identiek zijn met G.

§ 94. De Galois'sche groep van de algemeene *m*-*de* machtsvergelijking (welker wortels onafhankelijk veranderlijke grootheden zijn) is de symmetrische groep van *m* letters.

Want is weer $\varphi(\xi)$ de onontbindbare factor van $\Phi(\xi)$, die den wortel V bevat, dan krijgt men, als men in deze functie in Ω (welker coëfficienten dus functies der *c*'s zijn) de *c*'s door de wortels *a* vervangt en ook de V's in de *a*'s uitdrukt, eene functie der *a*'s, die nul is voor alle waarden der *a*'s, die men aan deze grootheden wil geven. Die functie is dus identiek nul; maar dan laat zij elke substitutie toe. Derhalve is $\varphi(V_i)$ nul voor elke waarde van i, dus is $\varphi(\xi)$ met $\Phi(\xi)$ identiek en is de vergelijking $\Phi(\xi) = 0$ onontbindbaar. De groep G omvat dus alle substituties $s, s_1, \ldots s_{m!-1}$.

In dit geval zegt Kronecker[1]), dat de vergelijking geen *affect* heeft.

§ 95. Is in een ander geval de graad van het Galois'sche lichaam n, een deeler van $m!$, dan heet $\frac{m!}{n}$ de graad van het affect der vergelijking.

---

[1]) Grundzüge einer arithm. Theorie der algebr. Grössen, bldz. 36).

Is het affect zoo groot mogelijk $m!$, dan is de graad der GALOIS'sche resolvente 1 en dan komen de wortels zelve in het lichaam Ω der coëfficienten voor.

Voor de oplossing eener vergelijking zal men er nu op uit moeten zijn, aan het lichaam der coëfficienten getallen toe te voegen, waardoor de GALOIS'sche resolvente in het uitgebreide lichaam ontbindbaar wordt. Daardoor neemt het affect der vergelijking toe en dit moet voortgezet worden tot de GALOIS'sche resolvente van den eersten graad wordt en het affect der vergelijking $m!$ is geworden.

§ 96. De eigenschappen der vergelijking spiegelen zich af in eigenschappen der groep [1]).

Eene ontbindbare vergelijking heeft b. v. eene intransitieve groep. Want is $f(x) = 0$ de onontbindbare factor van $F(x) = 0$, die van de m wortels $a, a_1, \ldots . a_{m-1}$ alleen de wortels $a, a_1, \ldots . a_{n-1}$ $(n < m)$ bevat, dan is $f(a) = 0$, zonder dat $f(a_i)$ nul is voor $i > n - 1$. In de groep der vergelijking kan dus volgens I (§ 92) geen substitutie voorkomen, die a in a_i overvoert. De groep is dus intransitief.

Weet men omgekeerd, dat de groep intransitief is, zoodat alle substituties van G de wortels $a, a_1, \ldots . a_{n-1}$ $(n < m)$ alleen onderling maar niet met de andere wortels kunnen verwisselen, dan blijft het product

$$(x - a)(x - a_1) \ldots . (x - a_{n-1})$$

door alle substituties van G onveranderd. Derhalve is het eene functie in Ω en is dus $F(x)$ ontbindbaar.

Eene vergelijking is dus al of niet ontbindbaar, al naar gelang haar groep intransitief of transitief is.

In verband met § 45 gevolg 4 is dus de orde van de groep eener onontbindbare vergelijking een veelvoud van den graad der vergelijking.

[1]) JORDAN, bldz. 259.

HOOFDSTUK VI.

Functiën der wortels van getallenvergelijkingen en ondergroepen der Galois'sche groep.

§ 97. In § 89 hebben we gezien, dat elke grootheid ω van 't lichaam $\Omega(a, a_1, \ldots\ldots a_{m-1})$ rationaal in de grootheid V uit te drukken is

$$\omega = \chi(V)$$

en dat elke toegevoegde grootheid ω_i (s_i is eene substitutie van de groep G van Galois) dezelfde functie is van V_i:

$$\omega_i = \chi(V_i).$$

Past men op deze laatste vergelijking in $\Omega(V)$ de substitutie s_j van G toe, dan blijft zij bestaan; derhalve:

$$(\omega_i)_j = \chi(V_{ij})$$

en dus

$$(\omega_i)_j = \omega_{ij}.$$

Past men dus op eene functie in $\Omega(V)$ achtereenvolgens twee substituties toe van de groep van Galois, dan krijgt men hetzelfde resultaat, als wanneer men het product der twee substituties op de functie toepast.

Hiermede is het bezwaar weggenomen in § 74 genoemd: de groep van Galois blijkt zoo te zijn voor functiën der wortels eener numerieke vergelijking wat de symmetri-

sche groep was voor functiën van onafhankelijk veranderlijke wortels eener algemeene vergelijking. De eigenschappen van Hoofdstuk III blijken dan ook door te gaan voor numerieke vergelijkingen, als men slechts de symmetrische groep vervangt door de groep van GALOIS en andere groepen, die ondergroepen waren van de symmetrische groep, door ondergroepen van de groep van GALOIS.

§ 98. Alle substituties van G, die eene grootheid ω van het lichaam Ω (V) onveranderd laten, vormen eene groep; en omgekeerd: bij elke groep g van G is eene grootheid van Ω (V) te vinden, die door deze substituties en door geen andere van G onveranderd blijft.

Bewijs. 1°. Past men op ω achtereenvolgens de substituties s_i en s_j toe, die ω onveranderd laten, dan vindt men $\omega_i = \omega$ en daarna $\omega_{ij} = \omega j = \omega$. De substitutie $s_i s_j$ laat dus ω ook onveranderd.

2°. Vormen de substituties

$$s_0 = 1, s_1, s_2, \ldots . s_{q-1}$$

eene ondergroep g van G, dan blijft

$$\omega = (\xi - V)(\xi - V_1)(\xi - V_2) \ldots . (\xi - V_{q-1})$$

onveranderd door alle substituties van g en door geen andere. Deze functie is niet de eenige, die door de substituties van g onveranderd blijft: men kan er elke symmetrische functie van $V, V_1, V_2, \ldots . V_{q-1}$ voor nemen.

Van de functie ω zegt men, dat zij bij de groep g, van de groep, dat zij bij de functie behoort.

§ 99. Is ν de index van eene ondergroep g in de groep G van GALOIS, en is ω eene functie der wortels, die bij g behoort, dan krijgt ω door alle verschillende substituties van G ν verschillende waarden.

Bewijs. Schrijf weer evenals in § 44 de substituties van G in rijen, waarvan g de eerste vormt.

Is $g = (s_0 = 1, s_1, s_2, \dots s_{q-1})$, dan is $\omega = \omega_{s_1} = \omega_{s_2} = \dots \omega_{s_{q-1}}$. Past men op deze vergelijking in V de substitutie σ_1 toe, dan krijgt men, daar $(\omega_{s_i})_{\sigma_1} = \omega_{s_i \sigma_1}$ is:

$$\omega_{\sigma_1} = \omega_{s_1 \sigma_1} = \omega_{s_2 \sigma_1} = \dots = \omega_{s_{q-1} \sigma_1}.$$

Evenzoo blijkt, dat alle substituties van elke volgende rij ω ook in een en dezelfde toegevoegde waarde overvoeren. Daar het aantal rijen ν is, is de stelling bewezen.

§ 100. Deze toegevoegde waarden

$$\omega, \omega_1, \omega_2, \dots \omega_{\nu-1}$$

zijn de wortels eener onontbindbare ν^{de}-machtsvergelijking in $\Omega(V)$:

$$(\xi - \omega)(\xi - \omega_1)(\xi - \omega_2) \dots (\xi - \omega_{\nu-1}) = 0.$$

De vergelijking is onontbindbaar, want *elke* vergelijking $r(\xi) = 0$ in $\Omega(V)$, die den wortel $\xi = \omega$ heeft, blijft bestaan, als men er de substituties van G op toepast, derhalve heeft die vergelijking ook de wortels $\omega_1, \omega_2, \dots \omega_{\nu-1}$.

§ 101. De stelling van LAGRANGE (§ 61) luidt nu: als eene functie Φ in $\Omega(V)$ onveranderd blijft door alle substituties van G, die eene andere functie φ in $\Omega(V)$ onveranderd laten (en misschien nog door andere substituties), dan is Φ rationaal in φ uit te drukken, m. a. w. Φ is dan een getal van het lichaam $\Omega(\varphi)$

't Bewijs is als vroeger.

§ 102. Gaan we nu na, wat er van het GALOIS'sche lichaam $\Omega(V)$ der vergelijking en van de GALOIS'sche groep G der vergelijking wordt, wanneer het oorspronkelijk lichaam Ω verruimd wordt door toevoeging van de eene of andere grootheid ε

De groep van de vergelijking in het nieuwe lichaam $\Omega(\varepsilon)$ wordt bepaald door den in 't nieuwe lichaam onontbindbaren factor van $\Phi(\xi)$, die den wortel V bevat. Deze factor heeft met den in 't lichaam Ω onontbind-

baren factor een wortel gemeen en al zijne wortels komen dus in den ouden factor voor. De groep wordt dus gevormd door een deel van de groep in 't oude lichaam.

Door toevoeging eener grootheid wordt de groep eener vergelijking dus gereduceerd tot eene ondergroep, die ondertusschen nog identiek kan zijn met de oorspronkelijke groep, wanneer de GALOIS'sche resolvente niet ontbindbaar wordt.

De oplossing van de vergelijking bestaat nu daarin, dat door achtereenvolgende toevoeging van grootheden aan het lichaam Ω, de GALOIS'sche resolvente teruggebracht wordt tot den eersten graad en de GALOIS'sche groep tot de identische groep. Het is nu dus eerst de vraag, door toevoeging van welke grootheden aan 't lichaam Ω, de GALOIS'sche resolvente werkelijk van lageren graad en de groep G dus kleiner wordt.

§ 103. Voegt men eene functie der wortels ω, die bij eene ondergroep g van G behoort, aan het lichaam Ω toe, dan wordt de GALOIS'sche groep der vergelijking gereduceerd tot de ondergroep g [1]).

Elke rationale functie in $\Omega(\omega)$ van de wortels der vergelijking, die eene grootheid van het lichaam $\Omega(\omega)$ is, blijft toch onveranderd door alle substituties van g (§ 92, I); en ook elke rationale functie der wortels, die onveranderd blijft door de substituties van g is volgens de stelling van LAGRANGE een getal van $\Omega(\omega)$.

§ 104. Zijn de substituties van de groep g

$$s_0 = 1,\ s_1,\ s_2, \ldots .\ s_{q-1}$$

dan is de onontbindbare factor, die zich van de GALOIS'sche resolvente

$$\varphi(\xi) = (\xi - V)(\xi - V_1) \ldots . (\xi - V_{n-1})$$

afsplitst door toevoeging van ω aan het lichaam Ω

$$(\xi - V)(\xi - V_{s_1})(\xi - V_{s_2}) \ldots . (\xi - V_{s_{q-1}}).$$

[1]) GALOIS, Oeuvres p. 42, proposition IV.

Schrijft men volgens § 44 de substituties van G in rijen

$$G = g + \tau_1 g + \tau_2 g + \ldots . \tau_{\nu-1} g$$

dan zal het product

$$(\xi - V_{\tau_i})(\xi - V_{\tau_i s_1})(\xi - V_{\tau_i s_2}) \ldots . (\xi - V_{\tau_i s_{q-1}})$$

onveranderd blijven door alle substituties van g en dus eene grootheid zijn van het lichaam $\Omega(\omega)$.

De GALOIS'sche resolvente splitst zich dus door toevoeging van ω aan 't lichaam Ω in ν factoren, die elk hetzelfde aantal wortels V_i bevatten [1]).

§ 105. De functie ω, door de toevoeging van welke de groep der vergelijking gereduceerd wordt tot de groep g, die in G den index ν heeft, moet echter eerst zelve bepaald worden uit eene resolvente van den ν^{den} graad. We zullen een stap nader gekomen zijn tot de oplossing van de vergelijking $F(x) = 0$, als wij er eerst in geslaagd zijn een wortel te vinden van de resolvente

$$r(\xi) \equiv (\xi - \omega)(\xi - \omega_1) \ldots . (\xi - \omega_{\nu-1}) = 0.$$

Om de oplosbaarheid dezer resolvente te beoordeelen, vormen we eerst haar GALOIS'sche groep Γ. Deze groep bestaat uit alle substituties der grootheden $\omega, \ldots . \omega_{\nu-1}$ die de rij

$$\omega, \omega_1, \omega_2, \ldots . \omega_{\nu-1} \qquad (\lambda)$$

overvoeren in de analoge rijen, die hieruit door de substituties van G ontstaan. De ω's zijn n. l. functiën van $a, a_1, \ldots . a_m$. Elke vergelijking tusschen de ω's blijft dus waar, als men op de a's de substituties van G toepast, d.i. als men op de ω's de genoemde substituties toepast. Laat eene functie van ω deze permutaties toe, dan blijft zij ook onveranderd door de substituties van G en is zij dus een getal van Ω.

Is de groep g in G eene alleenstaande ondergroep, dan

---

[1]) GALOIS. Oeuvres, p. 40, proposition II.

behoort zij bij alle waarden van ω en dan zullen alle q substituties van G, die in g voorkomen, geen verandering in de rij (λ) teweegbrengen.

Wordt de groep G dan geschreven

$$G = g + g\sigma_1 + g\sigma_2 + \ldots + g\sigma_{\nu-1}$$

(§ 49) dan voeren alle substituties $g\sigma_i$ de rij (λ) in éene en dezelfde rangschikking over. Daaruit blijkt, dat de groep Γ in dit geval isomorf is met G, terwijl met elke rij van g éene substitutie van G overeenkomt. Het aantal substituties van de groep Γ is dus $n : q = \nu$; en derhalve even groot als het aantal elementen, waarop de groep opereert.

Daar de groep bovendien transitief is, is zij in dit geval regelmatig.

§ 106. Is de index ν een priemgetal, dan wordt de groep G eene regelmatige groep van ondeelbare orde, derhalve de cyclische groep van ν elementen.

Het is de moeite waard, dit geval een beetje meer in 't bijzonder na te gaan. De groep G is, zooals reeds opgemerkt is, isomorf met Γ en met elke q substituties van G komt éene substitutie van Γ overeen. Alle q substituties, die in g voorkomen, komen overeen met de identische substitutie van Γ. Eene substitutie $g\sigma$, die niet in g voorkomt, komt overeen met eene substitutie τ van de cyclische groep Γ der orde ν. τ^ν, en geen lagere macht van τ, is de identische substitutie, dus is ook $(g\sigma)^\nu$ en geen lagere macht van $g\sigma$, eene substitutie van g Wat de orde van $g\sigma$ betreft, met eene macht van $g\sigma$, die de identische substitutie is, komt in Γ overeen eene macht τ, die de eenheid is. Deze laatste heeft tot exponent een veelvoud van ν; de orde van $g\sigma$ is dus ook een veelvoud van ν. Derhalve:

> als g eene alleenstaande ondergroep van G is van den ondeelbaren index ν, dan zal de νde macht, en geen lagere, van elke substitutie, die in G maar

niet in g voorkomt, eene substitutie van g zijn en de orde van elke substitutie van G, die niet in g voorkomt, is een veelvoud van ν.

§ 107. Is g geen alleenstaande ondergroep van G, maar hebben de gelijkstaande groepen

$$g, g_1, g_2, \ldots\ldots g_{\nu-1}$$

(die zeker de identische substitutie gemeen hebben) eene groep h gemeen, dan is dit (§ 51) zeker eene alleenstaande ondergroep van G. Heeft deze in G den index μ ($> \nu$), dan zullen telkens μ substituties van G de rij (λ) onveranderd laten. Met elke μ substituties van G komt dan éene substitutie van Γ overeen: de groep Γ zal dan $n:\mu$ substituties bevatten. De GALOIS'sche groep van de resolvente, die ω doet kennen, is dan dezelfde als de groep van de resolvente, waaruit te bepalen is eene functie, die behoort bij de grootst gemeene ondergroep der groepen $g, g_1, \ldots g_{\nu-1}$

In plaats van ω, die behoort bij de groep g, kan men dus met dezelfde moeite bepalen eene functie, die behoort bij de in G alleenstaande groep h. Door toevoeging van deze functie reduceert zich dan de GALOIS'sche groep tot de alleenstaande ondergroep h.

Resumeerende hetgeen in §§ 103—107 gebleken is, komen we dus tot het resultaat, dat reductie der groep kan verkregen worden, als men aan het lichaam Ω toevoegt eene functie der wortels, die in het lichaam $\Omega(a, a_1, \ldots a_{m-1})$ of Ω (V) voorkomt; elke mogelijke reductie door eene dergelijke toevoeging kan verkregen worden door de functie zoodanig te kiezen, dat de groep, die er bij behoort, eene alleenstaande ondergroep van G is.

§ 108. Het is nu de vraag, of reductie der groep ook kan plaats hebben door toevoeging eener algebraïsche grootheid ε, die niet in het lichaam Ω (V) voorkomt. Deze grootheid zal wortel zijn van eene in 't lichaam Ω onontbindbare vergelijking $\chi(\varepsilon) = 0$. Onderstellen we

bovendien deze vergelijking van ondeelbaren graad, dan kunnen wij bewijzen, dat ε tot het lichaam $\Omega\,(a, a_1, \ldots a_m)$ zal moeten behooren, wanneer door toevoeging van ε aan Ω reductie der groep zal kunnen ontstaan.

Laat toch door toevoeging van ε de GALOIS'sche resolvente gereduceerd worden tot den in $\Omega(\varepsilon)$ onontbindbaren factor

$$(\xi - V)(\xi - V_1) \ldots (\xi - V_{l-1}) = 0$$

dan bestaat de groep der vergelijking in 't lichaam $\Omega(\varepsilon)$ uit de substituties

$$s_0 = 1,\ s_1, \ldots\ s_{l-1}$$

die eene ondergroep g van G vormen, stel van den index j.

Laat nu φ eene functie in $\Omega(V)$ zijn, die bij deze groep g behoort dan zal

$$(\xi - V)(\xi - V_1) \ldots (\xi - V_{l-1})$$

volgens de stelling van LAGRANGE rationaal in φ zijn uit te drukken. Voegt men echter in plaats van ε de grootheid φ aan 't lichaam Ω toe, dan zal de onontbindbare factor van de GALOIS'sche resolvente ook

$$(\xi - V)(\xi - V_1) \ldots (\xi - V_{l-1})$$

worden. Derhalve zullen de coefficienten van dezen vorm zoowel rationale functiën van ε als rationale functiën van φ zijn:

$$\xi^l + r_1(\varepsilon)\,\xi^{l-1} + r_2(\varepsilon)\,\xi^{l-2} + \ldots + r_l(\varepsilon) =$$
$$= \xi^l + r'_1(\varphi)\,\xi^{l-1} + r'_2(\varphi)\,\xi^{l-2} + \ldots + r'_l(\varphi)$$

Deze vergelijking is identiek: men kan er voor ξ eene willekeurige waarde van Ω in schrijven. Vervangt men bovendien φ door u, dan wordt aan de vergelijking

$$\xi^l + r'_1(u)\,\xi^{l-1} + r'_2(u)\,\xi^{l-2} + \ldots + r'_l(u) -$$
$$- \left\{ \xi^l + r_1(\varepsilon)\,\xi^{l-1} + r_2(\varepsilon)\,\xi^{l-2} + \ldots + r_l(\varepsilon) \right\} = 0 \quad (\beta)$$

voldaan door $u = \varphi$. En daar de factor $(\xi - V) \ldots (\xi - V_{l-1})$ zeker niet gelijk is aan eenigen anderen factor der GALOIS'sche resolvente, zal aan deze vergelijking door geen der waarden $u = \varphi_1, \varphi_2, \ldots$ voldaan worden.

Derhalve zal de vergelijking (β) geen anderen wortel dan φ met de onontbindbare resolvente, $f(u) = 0$ [in 't lichaam $\Omega(\varphi)$] gemeen hebben. Zoekt men dus den grootst gemeenen deeler van den veelterm in (β) en $f(u)$, dan vindt men een lineairen vorm, waarin de bekende term eene functie van ε is. Deze moet voor $u = \varphi$ nul worden. Dus vindt men zoo φ in ε uitgedrukt. Derhalve komt φ in $\Omega(\varepsilon)$ voor. Volgens § 85 is dus de graad van het lichaam $\Omega(\varphi)$ een deeler van den graad van het lichaam $\Omega(\varepsilon)$. De graad van $\Omega(\varepsilon)$ is dus j of een veelvoud daarvan. Is echter $\chi(\varepsilon) = 0$ van ondeelbaren graad, dan kan die graad niet een veelvoud van j maar alleen j zelf zijn. Dan echter zijn de lichamen $\Omega(\varphi)$ en $\Omega(\varepsilon)$ identiek; ε is dan ook rationaal in φ uit te drukken: ε is dus een grootheid van het lichaam $\Omega(V)$.

KRONECKER noemt de grootheden van het GALOIS'sche lichaam $\Omega(V)$ eener vergelijking $F(x) = 0$ de natuurlijke irrationaliteiten der vergelijking. Boven is dus bewezen, dat *reductie der groep alleen verkregen kan worden door toevoeging eener natuurlijke irrationaliteit* [1]), wanneer ten minste de in Ω onontbindbare vergelijking, waarvan die grootheid de wortel is, van ondeelbaren graad is.

§ 109. We zijn nu voldoende voorbereid om de eischen voor de oplosbaarheid van eene vergelijking door de verruiming van het lichaam der coëfficienten nader te onderzoeken.

Wil men eene vergelijking oplossen door worteltrek-

---

[1]) WEBER, Algebra I, § 157. JORDAN, p. 270. Deze eigenschap is de uitbreiding van de stelling van ABEL, dat, als eene vergelijking oplosbaar is door worteltrekking, elke wortelgrootheid, die in de uitdrukking van de wortels voorkomt, rationaal kan worden uitgedrukt in de wortels en in eenheidswortels.

king, dan lost men telkens binomische resolventen op. En men kan het dan altijd zoo inrichten, dat deze binomische resolventen zijn van ondeelbaren graad.

Maar wanneer men zich beperkt tot de oplossing van resolventen van ondeelbaren graad en wortels dezer resolventen aan het lichaam der coefficienten toevoegt, dan krijgt men volgens § 107 alleen reductie der groep, wanneer de irrationaliteit, die men toevoegt eene natuurlijke is. De toe te voegen grootheden heeft men dus in 't GALOIS'sche lichaam $\Omega(a, a_1, \dots a_{m-1})$ of Ω (V) der vergelijking te zoeken. Maar de toevoeging van elke grootheid uit het lichaam Ω (V) kan zóó geschieden, dat de groep der vergelijking gereduceerd wordt tot eene alleenstaande ondergroep. En, wanneer de resolvente, waaruit men de toe te voegen grootheid moet vinden, van ondeelbaren graad is, zal de index der alleenstaande ondergroep in de groep van GALOIS een priemgetal zijn.

Voor de oplosbaarheid van de vergelijking blijkt het dus weer noodig te zijn, dat de groep van de vergelijking ontbonden kan worden zoo dat de achtereenvolgende alleenstaande ondergroepen in de voorgaande groep telkens een ondeelbaren aanwijzer hebben.

De samenstellingsfactoren van de GALOIS'sche groep der vergelijking moeten dus priemgetallen zijn.

Maar dan krijgt men nog de resolvente op te lossen, die de toe te voegen natuurlijke irrationaliteit zal doen kennen. Die resolvente heeft (in § 105 is 't gebleken) tot groep de cyclische groep. Het komt er dus nu op aan de oplossing te vinden van vergelijkingen met cyclische groep, d. i. van cyclische vergelijkingen.

HOOFDSTUK VII.

CYCLISCHE VERGELIJKINGEN [1]).

§ 110. Eene vergelijking heet cyclisch, als hare groep cyclisch is. De groep is dus b. v.

$$G = [s_0 = 1, s, s^2, \dots . s^{n-1}]$$

als $$s = (a, a_1, a_2 \dots . a_{n-1}) \text{ is.}$$

De cyclische groep is transitief, eene cyclische vergelijking is dus onontbindbaar.

De identische substitutie is de eenige substitutie der groep, die den wortel a onveranderd laat; zij laat ook a_1 onveranderd. Derhalve is volgens de stelling van LAGRANGE a_1 rationaal in a uit te drukken in het lichaam Ω:

$$a_1 = \varphi(a).$$

Deze vergelijking blijft echter bestaan, als men er de substituties der groep G op toepast. Derhalve

$$a_2 = \varphi(a_1), a_3 = \varphi(a_2), \dots a = \varphi(a_{n-1}).$$

Voert men de notaties

$$\varphi[\varphi(a)] = \varphi^2(a), \varphi[\varphi^2(a)] = \varphi^3(a), \dots . \text{ enz.}$$

in, dan wordt

$$a_1 = \varphi(a), a_2 = \varphi^2(a), a_3 = \varphi^3(a), \dots a = \varphi^n(a).$$

De in Ω rationale functie φ heeft dus de periode n en de wortels $a, a_1, a_2, \dots . a_{n-1}$ vormen een cyclus.

---

[1]) JORDAN, bldz. 286; WEBER, I, § 163.

§ 111. Omgekeerd is elke onontbindbare vergelijking, welker wortels op deze wijze een cyclus vormen, eene cyclische vergelijking.

Is toch $$a_k = \varphi^k(a) \quad (k = 0, 1, 2, \ldots.) \qquad (1)$$

en neemt men de indices daarbij gelijk als zij congruent zijn mod. n; is eene substitutie van de groep der vergelijking

$$s = \begin{pmatrix} a & a_1 & a_2 & \ldots. & a_{n-1} \\ a_i & a_{i_1} & a_{i_2} & \ldots. & a_{i_{n-1}} \end{pmatrix}$$

dan moet de vergelijking (1) waar blijven, als er deze substitutie op wordt toegepast. Derhalve

$$a_{i_k} = \varphi^k(a_i),$$

maar daar $a_i = \varphi^i(a)$ is, vindt men

$$a_{i_k} = \varphi^{i+k}(a) = a_{i+k}.$$

Derhalve is

$$i_k \equiv i + k \,(\text{mod. } n).$$

De substitutie s wordt dus:

$$s = \begin{pmatrix} a & a_1 & a_2 & \ldots. & a_{n-1} \\ a_i & a_{1+i} & a_{2+i} & \ldots. & a_{n-1+i} \end{pmatrix}.$$

Dit is echter de i^{de} macht van de substitutie

$$(a\, a_1\, a_2 \ldots.\, a_{n-1})$$

Derhalve behoort elke substitutie van de groep der vergelijking tot de cyclische groep. De groep der vergelijking is dus of de cyclische groep zelf of eene ondergroep daarvan: het laatste is echter onmogelijk omdat de vergelijking onontbindbaar ondersteld wordt en de groep dus transitief moet zijn.

§ 112. Is de graad der cyclische vergelijking ondeelbaar, dan is de groep der vergelijking enkelvoudig. Is de graad deelbaar, dan is de groep der vergelijking

samengesteld: de samenstellende reeks bevat dan geen andere dan cyclische groepen en de samenstellingsfactoren zijn de ondeelbare factoren van den graad der vergelijking (§ 70).

De oplossing van eene cyclische vergelijking van deelbaren graad is dus terug te brengen tot de oplossing van eene reeks cyclische vergelijkingen, alle van ondeelbaren graad.

We komen dus tot de oplossing van eene cyclische vergelijking van ondeelbaren graad p.

§ 113. Vorm daartoe de functie van LAGRANGE

$$V = a + \varepsilon a_1 + \varepsilon^2 a_2 + \ldots\ldots + \varepsilon^{p-1} a_{p-1}.$$

waarin ε eene complexe p^{de}-machtswortel der eenheid is.

Door de substitutie $s = (a\, a_1\, a_2 \ldots\ldots a_{p-1})$ gaat V over in ε^{-1} V; derhalve blijft V^p onveranderd door de substitutie s en dus door alle substituties van de groep G.

Maar dan blijft zij zeker onveranderd voor alle substituties van de groep G′, waartoe G gereduceerd kan zijn, nadat men ε aan 't lichaam Ω heeft toegevoegd. V^p is is dus een getal $r(\varepsilon)$ van 't lichaam $\Omega(\varepsilon)$ en V is door eene p^{de}-machtsworteltrekking te vinden:

$$V = \sqrt[p]{r(\varepsilon)}.$$

In V is elke wortel a_i dan weer uit te drukken.

§ 114. De uitdrukking voor a_i in V kan met behulp van eene door LAGRANGE aangegeven handelwijze [1]) gevonden worden.

De functie

$$V_i = a + \varepsilon^i a_1 + \varepsilon^{2i} a_2 + \ldots\ldots \varepsilon^{(p-1)i} a_{p-1}$$

gaat door de substitutie s ook over in $\varepsilon^{-i} V_i$; derhalve blijft V_i^p ook onveranderd voor alle substituties der groep en in dus V_i^p een getal $r_i(\varepsilon)$ van het lichaam $\Omega(\varepsilon)$.

---

[1]) Réflexions sur la résolution algébrique des équations; section 3me, no. 67 (Nouveaux Mém. de l'Acad. Royale de Berlin, 1770. p. 162).

Substitueeren we nu achtereenvolgens voor i de waarden *1, 2, ... p—1*, dan vinden we dus:

$$a + \varepsilon a_1 + \varepsilon^2 a_2 + \ldots + \varepsilon^i a_i + \ldots + \varepsilon^{p-1} a_{p-1} = \sqrt[p]{r_1(\varepsilon)}$$

$$a + \varepsilon^2 a_1 + \varepsilon^4 a_2 + \ldots + \varepsilon^{2i} a_i + \ldots + \varepsilon^{2(p-1)} a_{p-1} = \sqrt[p]{r_2(\varepsilon)}$$

. . . .

$$a + \varepsilon^{p-1} a_1 + \varepsilon^{2(p-1)} a_2 + \ldots + \varepsilon^{i(p-1)} a_i + \ldots + \\ + \varepsilon^{(p-1)^2} a_{p-1} = \sqrt[p]{r_{p-1}(\varepsilon)}.$$

Voegt men hierbij de vergelijking

$$a + a_1 + a_2 + \ldots + a_i + \ldots + a_{p-1} = c_1$$

dan heeft men p lineaire vergelijkingen met p onbekenden.

Daar ε, ε^2, ... de wortels zijn van de vergelijking

$$1 + x + x^2 + \ldots + x^{p-1} = 0$$

is

$$1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{p-1} = 0$$

$$1 + \varepsilon^2 + \varepsilon^4 + \ldots + \varepsilon^{2(p-1)} = 0$$

enz.

Derhalve kan men a_i vinden door de eerste vergelijking te vermenigvuldigen met ε^{-i}, de 2de met ε^{-2i}, ... de $p - 1$ste met $\varepsilon^{-(p-1)i}$ en al deze vergelijkingen vervolgens bij de laatste op te tellen. Men vindt dan

$$p a_i = c_1 + \varepsilon^{-i} \sqrt[p]{r_1(\varepsilon)} + \varepsilon^{-2i} \sqrt[p]{r_2(\varepsilon)} + \ldots + \\ \varepsilon^{-(p-1)i} \sqrt[p]{r_{p-1}(\varepsilon)}.$$

Stelt men voor i achtereenvolgens 0, 1, 2, ... $p - 1$ dan krijgt men alle waarden a, a_1, $a_2 \ldots a_{p-1}$.

In de uitdrukkingen voor de wortels komen $p - 1$ wortelgrootheden voor, die alle p-waardig zijn. Voor een dier wortelgrootheden kan men onder de p waarden eene willekeurige kiezen: de andere zijn dan bepaald, daar $\sqrt[p]{r_i(\varepsilon)} : \left[\sqrt[p]{r_1(\varepsilon)}\right]^i$ door geen enkele substitutie van G van waarde verandert en dus een getal van $\Omega(\varepsilon)$ is.

Door het aannemen van eene waarde voor $\sqrt[p]{r_1(\varepsilon)}$, is dus meteen beslist welke waarde van $\sqrt[p]{r_i(\varepsilon)}$ genomen moet worden.

§ 115. De oplossing der cyclische vergelijkingen van ondeelbaren graad p, en daarmede die van cyclische vergelijkingen van deelbaren graad, is dus tot een goed einde gebracht, wanneer men er ten minste eerst in geslaagd is een wortel ε te vinden van de vergelijking

$$x^{p-1} + x^{p-2} + \ldots . + x^2 + x + 1 = 0 \qquad (2)$$

de zoogenaamde vergelijking voor de cirkelverdeeling. Stelt men zich toch in het vlak der complexe grootheden den cirkel met den eenheidsstraal voor, die den oorsprong tot middelpunt heeft, dan zijn de wortels dezer vergelijking de punten in 't complexe vlak, die den cirkel in p gelijke deelen verdeelen, als men er het punt, waar de cirkel de positieve x-as snijdt, bij neemt.

De vergelijking voor de cirkelverdeeling is 't eerst door GAUSS opgelost. [1])

§ 116. Voor het geval, dat p een oneven priemgetal is, het eenige geval, waarmee we hier te maken hebben, is de vergelijking (2) in het lichaam Ω der rationale getallen onontbindbaar.

Bewijs. Vooraf moge gaan de volgende hulpstelling: als $F(x)$, eene geheele functie van x met geheele coëfficienten en waarin de coëfficient van de hoogste macht van x de eenheid is, een rationalen deeler $f(x)$ heeft, waarin de coëfficient der hoogste macht van x de eenheid is, zijn alle andere coëfficienten van $f(x)$ geheele getallen. [2])

Onderstellen we, dat in

$$\mathrm{F}(x) = f(x) \,.\, \varphi(x)$$

onder de coëfficienten van $f(x)$ breuken voorkomen, in

---

[1]) Disquisitiones arithmeticae, sectio VII, art. 336—366.

[2]) JORDAN, p. 294.

welker noemers, nadat zij zooveel mogelijk verkleind zijn, de ondeelbare factor q gevonden wordt. Zij de term cx^m in $f(x)$ zóó gekozen, dat q in den noemer van c voorkomt tot eene hoogere macht dan in de coëfficienten der vorige termen en tot eene niet lagere macht dan in de coëfficienten der volgende termen. Zij dx^n de term, waarvoor hetzelfde geldt in $\frac{\varphi(x)}{q}$, waarin de noemer q ten minste in den eersten term voorkomt. Vormt men dan in het product $f(x) \times \frac{\varphi(x)}{q}$ de termen met x^{m+n} dan zal onder deze termen voorkomen die met de coëfficient cd, die ten minste q^2 in den noemer heeft. En de macht van q in den noemer van cd zal hooger zijn dan die in den noemer van eenigen anderen term x^{m+n}. Worden deze termen samengenomen, dan zal dus minstens de 2de macht van q in den noemer van deze coëfficient blijven. In het product $f(x) \times \varphi(x)$ zal de term x^{m+n} dus minstens één factor q in den noemer der coëfficient hebben, hetgeen strijdt met het ondersteIde, dat $F(x)$ geheele getallen als coëfficienten heeft.

§ 117. Stel nu, om te bewijzen, dat

$$F(x) \equiv x^{p-1} + x^{p-2} + \dots x + 1$$

onontbindbaar [1]) is, dat $F(x)$ in 2 factoren $f(x)$ en $\varphi(x)$ te ontbinden was, waarin de coëfficienten van de termen der hoogste machten van x zonder aan de algemeenheid te kort te doen, gelijk 1 ondersteld kunnen worden. Dan zouden volgens de hulpstelling $f(x)$ en $\varphi(x)$ geheele getallen als coëfficienten moeten hebben. Maar dan zou, als men $x = 1$ stelt,

$$f(1) \,.\, \varphi(1) = p$$

worden. Eén dezer factoren b.v. $f(1)$ zou dan ± 1 moeten zijn. Daar deze factor $f(x)$ met $F(x)$ minstens één wortel

[1]) NETTO, bldz. 174.

ε gemeen heeft en alle andere wortels van $F(x)$ geschreven kunnen worden $\varepsilon^2, \varepsilon^3, \ldots \varepsilon^{p-1}$, zou dan de vergelijking

$$f(x) \cdot f(x^2) \cdot f(x^3) \ldots\ldots f(x^{p-1}) = 0$$

zeker alle wortels van $F(x)$ hebben. Het eerste lid dezer vergelijking zou dan ontbindbaar zijn:

$$f(x) \cdot f(x^2) \cdot f(x^3) \ldots\ldots f(x^{p-1}) = F(x) \times \chi(x)$$

en $\chi(x)$ zou dan volgens de hulpstelling weer geheele getallen als coëfficienten hebben. Maar dan zou men vinden door $x = 1$ te stellen:

$$[f(1)]^{p-1} = p \times \chi(1)$$

Daar $f(1) = \pm 1$ was, en χ geheele coëfficienten heeft, is dit onmogelijk. Derhalve is $F(x)$ onontbindbaar in 't lichaam der rationale getallen.

§ 118. Van de vergelijking (2) kan men nu gemakkelijk laten zien, dat zij cyclisch is. Immers zij is onontbindbaar en hare wortels zijn

$$\varepsilon, \varepsilon^2, \varepsilon^3, \ldots\ldots \varepsilon^{p-1}.$$

Is echter g een primitieve wortel van den modulus p, is dus g een getal, waarvan de machten

$$g^0, g^1, g^2, \ldots\ldots g^{p-2}$$

incongruent zijn (mod. p), dan zijn deze machten op de volgorde na congruent (mod. p) met de getallen

$$1, 2, 3, \ldots\ldots p-1.$$

De $p-1$ wortels kunnen dus ook voorgesteld worden door

$$\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \ldots\ldots \varepsilon^{g^{p-2}}.$$

Stelt men dus $\varepsilon^g = \varphi(\varepsilon)$, dan zijn de wortels te schrijven:

$$\varepsilon, \varphi(\varepsilon), \varphi^2(\varepsilon), \ldots\ldots \varphi^{p-2}(\varepsilon).$$

Volgens § 111 is de vergelijking (2) eene cyclische vergelijking.

§ 119. De oplossing van eene cyclische vergelijking van ondeelbaren graad p bleek afhankelijk te zijn van de oplossing van de vergelijking der cirkeldeeling van den graad $p-1$. Maar dit blijkt weer eene cyclische vergelijking te zijn, welker oplossing terug te brengen is tot de oplossing van cyclische vergelijkingen, welker graden de ondeelbare factoren van $p-1$ zijn.

Het vraagstuk van de oplossing eener cyclische vergelijking van ondeelbaren graad is daarmede tot een eenvoudiger vraagstuk teruggebracht: dit vraagstuk op dezelfde wijze behandelende, blijkt de oplossing der cyclische vergelijkingen terug te brengen te zijn tot de oplossing van eene cyclische vergelijking van den 2den graad.

Elke cyclische vergelijking kan dus door algebraïsche bewerkingen worden opgelost.

§ 120. Als een belangrijk voorbeeld van de vergelijkingen voor de cirkelverdeeling schetsen we iets meer uitvoerig de oplossing voor het geval $p-1$ geen andere factoren dan 2 bevat. De samenstellingsfactoren van de samengestelde cyclische groep zijn dan alle 2 en voor de oplossing van de vergelijking heeft men geen andere resolventen dan van den 2den graad. Het meetkundige vraagstuk kan in dit geval, daar er geen andere wortels dan vierkantswortels optreden, met behulp van passer en lineaal opgelost worden. Het geval doet zich dus voor, als p priem is en $p-1$ alleen factoren 2 bevat, dus $p=2^m+1$. Dit getal kan niet priem zijn dan wanneer m geen enkelen oneven factor bevat; want was $m=m'\mu$ (μ oneven), dan zou $2^{m'\mu}+1$ deelbaar zijn door $2^{m'}+1$. Het getal m moet dus zeker zijn van den vorm 2^n, zoodat $p=2^{2^n}+1$ moet zijn. Niet elk getal van deze gedaante is echter ondeelbaar: $2^{2^5}+1=641\times 6700417$,

$2^{2^{12}}+1$ is door 114689, $2^{2^{23}}+1$ door 167772161 deelbaar [1]).

§ 121. Behandelen we nu als voorbeeld het geval van den zeventienhoek:

$$x^{16}+x^{15}+\ldots\ldots+x^2+x+1=0. \qquad (3)$$

De wortels $\varepsilon, \varepsilon^2, \ldots\ldots \varepsilon^{15}, \varepsilon^{16}$ zijn in één cyclus te schrijven. Voor $p=17$ is $g=3$ een primitieve wortel.

De wortels der vergelijking

$$a, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16},$$

worden dus, als elk de 3de macht is van de voorgaande:

$$\varepsilon, \varepsilon^3, \varepsilon^9, \varepsilon^{10}, \varepsilon^{13}, \varepsilon^5, \varepsilon^{15}, \varepsilon^{11}, \varepsilon^{16}, \varepsilon^{14}, \varepsilon^8, \varepsilon^7, \varepsilon^4, \varepsilon^{12}, \varepsilon^2, \varepsilon^6.$$

Is nu s de substitutie

$$s=(\varepsilon\, \varepsilon^3\, \varepsilon^9\, \varepsilon^{10}\, \varepsilon^{13}\, \varepsilon^5\, \varepsilon^{15}\, \varepsilon^{11}\, \varepsilon^{16}\, \varepsilon^{14}\, \varepsilon^8\, \varepsilon^7\, \varepsilon^4\, \varepsilon^{12}\, \varepsilon^2\, \varepsilon^6),$$

dan is de groep der vergelijking:

$$G=(s, s^2, s^3, s^4, s^5, s^6, s^7, s^8, s^9, s^{10}, s^{11}, s^{12}, s^{13}, s^{14}, s^{15}, s^{16}=1).$$

Deze groep ontbinden we als volgt:

$$g_1=(s^2, s^4, s^6, s^8, s^{10}, s^{12}, s^{14}, s^{16}=1)$$

$$g_2=(s^4, s^8, s^{12}, s^{16}=1)$$

$$g_3=(s^8, s^{16}=1)$$

$$g_4=(s^{16}=1)$$

Als functie van $\Omega(V)$, d. i. hier dus van $\Omega(\varepsilon)$, die behoort bij de ondergroep g_1 kunnen we nemen

$$\varphi_1=\varepsilon+\varepsilon^9+\varepsilon^{13}+\varepsilon^{15}+\varepsilon^{16}+\varepsilon^8+\varepsilon^4+\varepsilon^2.$$

De in G hieraan toegevoegde functie is

$$\varphi_1'=\varepsilon^3+\varepsilon^{10}+\varepsilon^5+\varepsilon^{11}+\varepsilon^{14}+\varepsilon^7+\varepsilon^{12}+\varepsilon^6.$$

---

[1]) NETTO, bldz. 181.

Daar g_1 eene alleenstaande groep in G is van ondeelbaren index, zal de resolvente, die de functiën φ_1 en φ'_1 doet kennen, eene cyclische vergelijking zijn en wel in dit geval eene cyclische vergelijking van den 2den graad. De 2de-machtswortels der eenheid zijn echter + 1 en — 1; de cyclische functie voor φ_1 en φ'_1 wordt dus $\varphi_1 - \varphi'_1$ en de 2de macht dezer functie blijkt werkelijk eene grootheid in Ω te zijn. Want, daar $\varphi_1 + \varphi'_1 = -1$ en $\varphi_1 \varphi'_1 = -4$ is, vindt men

$$(\varphi_1 - \varphi'_1)^2 = 17.$$

Hieruit kan men φ_1 en φ'_1 vinden. Voegt men nu φ_1 en daarmede tevens φ'_1 aan 't lichaam Ω toe, dan reduceert zich de groep der vergelijking tot g_1.

g_2 is nu eene alleenstaande ondergroep van index 2. Voor de functie, die er bij behoort, kan men kiezen

$$\varphi_2 = \varepsilon + \varepsilon^{18} + \varepsilon^{16} + \varepsilon^4 \quad \text{of} \quad \psi_2 = \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12}$$

waarvan de in g_1 toegevoegde functiën zijn:

$$\varphi'_2 = \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 + \varepsilon^2 \quad \text{en} \quad \psi'_2 = \varepsilon^{10} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^6.$$

Voor de cyclische resolventen vindt men in de 2 gevallen:

$$(\varphi_2 - \varphi'_2)^2 = \varphi_1^2 + 4$$

en

$$(\psi_2 - \psi'_2)^2 = \varphi_1'^2 + 4$$

daar:

$$\begin{matrix} \varphi_2 + \varphi'_2 = \varphi_1 \\ \varphi_2 \cdot \varphi'_2 = -1 \end{matrix} \quad \text{en} \quad \begin{matrix} \psi_2 + \psi'_2 = \varphi'_1 \\ \psi_2 \cdot \psi'_2 = -1. \end{matrix}$$

Heeft men nu φ_2 opgelost en aan $\Omega(\varphi_1)$ toegevoegd en daarmede ook φ'_2, ψ_2 en ψ'_2 (want volgens de stelling van LAGRANGE is ook ψ_2 rationaal in φ_2 uit te drukken), dan is de groep g_1 gereduceerd tot de groep g_2.

Nu is weer g_3 eene alleenstaande ondergroep van index

2 in g_2. Voor de functie, die bij g_3 behoort, kan men nemen

$$\varphi_3 = \varepsilon + \varepsilon^{16}.$$

De toegevoegde functie in g_2 is

$$\varphi_3' = \varepsilon^4 + \varepsilon^{13}.$$

Daar nu $\varphi_3 + \varphi_3' = \varphi_2$ en $\varphi_3 \varphi_3' = \psi_2$ is, vindt men voor de cyclische resolvente voor φ_3:

$$(\varphi_3 - \varphi_3')^2 = \varphi_2^2 - 4\,\psi_2.$$

Lost men φ_3 op en voegt die toe aan het lichaam $\Omega(\varphi_1, \varphi_2)$ dan reduceert zich de groep der vergelijking tot g_4, die alleen uit de eenheid bestaat. Kiest men als functie, die bij de groep g_4 behoort:

$$\varphi_4 = \varepsilon$$

dan is de in g_3 toegevoegde functie hiervan $\varphi_4' = \varepsilon^{16}$ en daar $\varphi_4 + \varphi_4' = \varphi_3$ en $\varphi_4 . \varphi_4' = 1$ is, vindt men voor de cyclische resolvente voor φ_4:

$$(\varphi_4 - \varphi_4')^2 = \varphi_3^2 - 4.$$

Hieruit kan men φ_4 vinden en daarmee is ε en zijn dus alle wortels van de vergelijking (3) bepaald.

§ 122. De cyclische vergelijkingen vormen een bijzonder geval van eene algemeene klasse van vergelijkingen, de Abelsche vergelijkingen. Eene onontbindbare vergelijking heet eene Abelsche, als alle wortels er van rationaal door één hunner zijn uit te drukken:

$$a_1 = \varphi_1(a) \quad a_2 = \varphi_2(a) \quad \ldots\ldots \quad a_{n-1} = \varphi_{n-1}(a)$$

en als deze functiën $\varphi_1, \varphi_2, \ldots\ldots \varphi_{n-1}$ zóo zijn, dat

$$\varphi_i[\varphi_j(a)] = \varphi_j[\varphi_i(a)] \qquad \text{is.}$$

Dat de cyclische vergelijkingen hiertoe behooren, is duidelijk. Op de volgende wijze ziet men gemakkelijk in, dat zij slechts een bijzonder geval zijn. Is

$$a_1 = \varphi(a)$$

dan zal men op deze vergelijking de substituties der groep G mogen toepassen. De groep is transitief, omdat de vergelijking onontbindbaar is Er is dus eene substitutie, die a in a_1 overvoert; bevat deze den cyclus

$$(a\, a_1\, a_2 \ldots\ldots a_{l-1})$$

dan vindt men dus:

$$a_2 = \varphi(a_1),\quad a_3 = \varphi(a_2)\ ,\ldots\ a_{l-1} = \varphi(a_{l-2}),\quad a = \varphi(a_{l-1})$$

en dus

$$a_2 = \varphi^2(a_1),\quad a_3 = \varphi^3(a)\ ,\ldots\ldots\ a_{l-1} = \varphi^{l-1}(a),\quad a = \varphi^l(a)$$

Maar met deze wortels behoeft het totale aantal wortels niet te zijn uitgeput. Er is dan eene substitutie in de groep, die a vervangt door een wortel a', die niet voorkomt in de reeks $a, a_1, a_2, \ldots\ldots a_{l-1}$. Voert deze substitutie meteen $a_1, a_2, \ldots\ldots a_{l-1}$ resp. over in $a'_1, a'_2, \ldots\ldots a'_{l-1}$, dan vindt men ook

$$a'_1 = \varphi(a'),\ a'_2 = \varphi^2(a')\ \ldots\ldots\ a'_{l-1} = \varphi^{l-1}(a').$$

Is hiermee het geheele aantal wortels nog niet uitgeput dan kan men nog meer reeksen wortels krijgen, die op dezelfde wijze samenhangen.

§ 123. De groep van eene Abelsche vergelijking is in het algemeen imprimitief: de wortels van eene zelfde reeks worden of alle onderling verwisseld, of zij worden alle verwisseld met wortels, die tot éene en dezelfde andere reeks behooren.

De groep is bovendien commutatief en van elke onontbindbare vergelijking met commutatieve groep kan bewezen worden, dat zij eene Abelsche is.

Keeren we echter terug tot de algebraïsche oplosbaarheid van eene willekeurige vergelijking.

HOOFDSTUK VIII.

Oplosbaarheid door wortelgrootheden.

§ 124. Overzien we nu eens, waartoe wij gekomen zijn. Als een vergelijking algebraïsch opgelost is, heeft men de wortels met behulp van algebraïsche bewerkingen in de coëfficienten der vergelijking uitgedrukt. Om de wortelgrootheden, in deze uitdrukkingen voorkomende, te bepalen, heeft men (binomische) resolventen moeten oplossen, welker graden men zonder aan de algemeenheid te kort te doen, ondeelbaar mocht onderstellen.

Aanvankelijk zijn dus alleen de getallen van het lichaam Ω, dat ontstaat uit de coëfficienten der vergelijking, bekend; door toevoeging van functiën, die door oplossing van resolventen van ondeelbaren graad gevonden worden, is dit lichaam ten slotte zoodanig uitgebreid, dat in het nieuwe lichaam Ω' de wortels der vergelijking voorkomen.

Om te beoordeelen of de uitbreiding van het lichaam Ω ver genoeg is gevorderd, kan men gebruik maken van de eigenschappen van de Galois'sche groep der vergelijking: eene grootheid behoort tot het lichaam Ω, als zij onveranderd blijft door alle substituties van de groep G der vergelijking. Zullen dus de wortels in een uitgebreid lichaam Ω' voorkomen, dan moeten zij onveranderd blijven door alle substituties der groep G. Maar,

daar alle wortels der vergelijking ondersteld worden te verschillen, zullen alle substituties, die de wortels onveranderd laten, bestaan in de identische substitutie alleen en de groep der vergelijking moet dus, als de wortels in het lichaam Ω' voorkomen, bestaan uit de eenheid alleen.

Het vraagstuk van de uitbreiding van het lichaam Ω tot dat de wortels er in voorkomen, gaat dus hand in hand met het vraagstuk van de reductie der GALOIS'sche groep tot de eenheid.

Bij de algebraïsche oplossing der vergelijking wordt het lichaam Ω alleen uitgebreid door toevoeging van wortels van resolventen van ondeelbaren graad. Wil eene dergelijke toevoeging reductie van de groep ten gevolge hebben, dan moet volgens § 108 de toe te voegen grootheid eene natuurlijke irrationaliteit zijn, d. w. z. eene grootheid van het lichaam $\Omega(a, a_1, a_2 \ldots.)$, dat uit 't lichaam Ω van de coëfficienten gevormd wordt door toevoeging van alle wortels.

En als zulk eene grootheid wordt toegevoegd, reduceert zich de groep (§ 107) tot eene alleenstaande ondergroep. Ter bepaling van de toe te voegen grootheid moet eene resolvente opgelost worden, die wij, zooals gezegd is, bij de algebraïsche oplossing eener vergelijking altijd van ondeelbaren graad kunnen onderstellen. Die resolvente wordt echter bij de bepaling van eene functie die bij eene alleenstaande groep behoort, alleen dan van ondeelbaren graad, als de index van de alleenstaande ondergroep een priemgetal is En het feit, dat de index ondeelbaar is, maakt (§ 106) de resolvente weer tot eene cyclische vergelijking, die blijkens het vorige Hoofdstuk algebraïsch is op te lossen.

Voor de algebraïsche oplosbaarheid eener vergelijking wordt dus geëischt, dat de aan het lichaam toe te voegen functie behoort bij eene alleenstaande ondergroep van ondeelbaren aanwijzer in G en daar bij elke groep eene functie gevonden kan worden, komt de eisch daarop

neer, dat in de groep G eene alleenstaande ondergroep g van ondeelbaren aanwijzer te vinden is.

Maar voor de verdere reductie is nu weer noodig, dat in g eene alleenstaande ondergroep van priem index voorkomt. Zoo voortgaande moet men ten slotte komen tot de eenheidsgroep.

De eenige eisch voor de algebraïsche oplosbaarheid eener vergelijking is dus, dat de samenstellingsfactoren van de GALOIS'sche groep der vergelijking priemgetallen zijn. Want ook als dit het geval is, worden blijkens het voorgaande alle resolventen cyclische vergelijkingen van ondeelbaren graad en deze kunnen volgens het vorige hoofdstuk algebraïsch opgelost worden.

We komen dus tot de volgende stelling van GALOIS: **Opdat eene vergelijking algebraïsch oplosbaar zij, is het noodig en voldoende, dat de samenstellingsfactoren harer groep alle priemgetallen zijn.**

§ 125. De groep der n.de-machtsvergelijking, welker coëfficiënten onafhankelijk veranderlijke grootheden zijn, is (§ 94) de symmetrische groep van m letters. Deze heeft tot samenstellingsfactoren (§ 73) 2 en $\frac{m!}{2}$, als ten minste $m > 4$ is. De algemeene $m$de-machtsvergelijking is dus voor $m > 4$ onoplosbaar door wortelgrootheden.

§ 126. Beperken we ons nu tot vergelijkingen van ondeelbaren graad en zoeken we de algemeenste onontbindbare vergelijking van ondeelbaren graad p, die door algebraïsche bewerkingen oplosbaar is.

De groep van zulk eene vergelijking is transitief (§ 96) en dus is hare orde deelbaar door haar graad p (§ 45). Volgens de stelling van CAUCHY bevat zij dus eene cyclische substitutie $\sigma = (a\, a_1\, a_2 \ldots a_{p-1})$ van de orde p. Deze substitutie zal in de eerste groepen der samenstellende reeks

$$G, g_1, g_2, \ldots 1$$

voorkomen, in volgende groepen niet meer. Laat g_i de

substitutie nog bevatten, g_{i+1} niet meer. Van alle machten van σ kan dan alleen de eenheid in g_{i+1} voorkomen; maar de laagste macht van σ, die de eenheid is, is de p^{de}. Daartoe zal volgens § 106 de index van g_{i+1} in g_i gelijk aan p moeten zijn.

Laat nu s eene substitutie van g_{i+1} zijn, die van de eenheid verschilt en die b.v. a_l in a_m overvoert; σ^{l-m} vervangt a_m door a_l, derhalve zal $s\sigma^{l-m}$ de letter a_l onveranderd laten. Deze substitutie zal wel in g_i maar niet in g_{i+1} voorkomen, omdat σ niet in g_{i+1} voorkomt; derhalve zal weer volgens § 106 de orde van $s\sigma^{l-m}$ een veelvoud van p moeten zijn. Maar dit is onmogelijk, omdat $s\sigma^{l-m}$ niet alle p letters verplaatst en het kleinst gemeene veelvoud van de orden harer cycli dus geen factor p kan bevatten.

De groep g_{i+1} kan dus niet anders zijn dan de identische groep [1]).

§ 127. Bouwen we nu de samenstellende reeks op, te beginnen met de identische groep; g_i, die daaraan voorafgaat, moet de cyclische groep van de orde p zijn, omdat de index van $g_{i+1} = 1$ in g_i gelijk aan p is. Maar dan moet volgens § 52 g_{i-1} de metacyclische groep of een van hare ondergroepen zijn en g_{i-1} bevat dan, blijkens hetgeen daar ter plaatse gezegd is, geen andere cyclische substituties van de orde p, dan die in g_i voorkomen.

g_{i-2} zal g_{i-1} als alleenstaande ondergroep van ondeelbaren index bevatten, maar ook g_i zal in g_{i-2} eene alleenstaande ondergroep zijn, want als men eene substitutie σ van g_i door eene substitutie van g_{i-2} transformeert, dan zal de getransformeerde, die weder eene cyclische substitutie der orde p is, behooren tot g_{i-1}, omdat σ tot g_{i-1} behoort en g_{i-1} in g_i eene alleenstaande ondergroep is; maar g_{i-1} bevat geen andere cyclische

[1]) Bolza. Am. Journ. of Math, XIII, bldz. 141.

substituties der orde p dan die tot g_i behooren. Derhalve is de substitutie, die ontstaat als men σ (van g_i) transformeert door eene substitutie van g_{i-2}, weer eene substitutie van g_i en is dus g_i eene alleenstaande ondergroep van g_{i-2}.

Maar dan behoort ook g_{i-2} tot de metacyclische groep van p letters. Evenzoo kan men bewijzen, dat de volgende groepen g_{i-3} g_{i-4}, ... en dus eindelijk G behooren tot de metacyclische groep van p letters. Zoo vindt men dus de volgende stelling van GALOIS: [1])

Elke onontbindbare vergelijking van ondeelbaren graad, die algebraïsch oplosbaar is, heeft tot groep de metacyclische groep of een van hare transitieve ondergroepen.

§ 128. Omgekeerd is ook elke vergelijking van ondeelbaren graad, die tot groep heeft de metacyclische groep of een harer transitieve ondergroepen, algebraïsch oplosbaar.

Nemen we eerst eene vergelijking met de metacyclische groep. De cyclische groep van p letters is eene alleenstaande ondergroep. Eene functie φ, hierbij behoorende, wordt gevonden uit eene resolvente van den $(p-1)$sten graad, omdat $p-1$ de index is van de cyclische groep. De $p-1$ waarden van φ kunnen, blijkens de 2de rangschikking van de substituties der metacyclische groep, die in § 54 gegeven is, gerangschikt worden in een cyclus

$$\varphi \quad \varphi_g \quad \varphi_{g^2} \ldots . \quad \varphi_{g^{p-2}}.$$

De resolvente is dus blijkens § 111 eene cyclische vergelijking: zij is dus algebraïsch op te lossen.

Voegt men dan φ toe aan het lichaam Ω, dan reduceert zich de groep van de vergelijking tot de groep, die bij φ behoort, d. w. z. tot de cyclische ondergroep der orde p Maar dan is de vergelijking eene cyclische geworden: zij is dus ook algebraïsch oplosbaar.

---

[1]) GALOIS. Oeuvres, p. 48

Op dezelfde wijze toont men aan, dat eene onontbindbare vergelijking van ondeelbaren graad algebraïsch oplosbaar is, als haar groep eene ondergroep van de metacyclische groep is.

§ 129. Noemt men eene onontbindbare vergelijking van ondeelbaren graad, die tot groep heeft de metacyclische groep of eene van hare ondergroepen, eene *metacyclische* vergelijking, dan is dus gebleken **dat elke metacyclische vergelijking algebraïsch oplosbaar is en dat elke algebraïsch oplosbare vergelijking metacyclisch is.**

§ 130. Tusschen de wortels eener metacyclische vergelijking bestaat een merkwaardig verband: de identische substitutie is n.l. de eenige substitutie der groep, die de functie $\lambda a + \lambda_1 a_1$ onveranderd laat, want geen enkele andere substitutie der metacyclische groep laat meer dan éen letter onveranderd; volgens de stelling van LAGRANGE is dus elke wortel rationaal uit te drukken in deze functie, dus ook in a en a_1. [1])

Omgekeerd, als een onontbindbare vergelijking van ondeelbaren graad zóo is, dat elke wortel in het lichaam Ω rationaal is uit te drukken in twee der wortels, b.v. in a en a_1:

$$a_i = \varphi_i (a, a_1)$$

dan zal de groep zoodanig moeten zijn, dat deze betrekking door de substituties der groep onaangetast wordt gelaten. Maar dan kan in de groep geen enkele substitutie voorkomen, die de 2 letters a en a_1 onveranderd laat en eene andere letter omzet, want dan zou de vergelijking gelijke wortels krijgen en dus ontbindbaar worden. Onder de substituties der groep mag er dus geen enkele zijn, die twee letters onveranderd laat. De groep is dus (§ 53) de metacyclische groep of een harer transitieve ondergroepen.

§ 131. Noemt men eene onontbindbare vergelijking

[1]) GALOIS, Oeuvres, p. 49.

van ondeelbaren graad, welker wortels rationaal in twee hunner zijn uit te drukken, eene *vergelijking van* GALOIS, dan is dus bewezen, dat **elke vergelijking van Galois algebraïsch oplosbaar is en dat elke oplosbare onontbindbare vergelijking van ondeelbaren graad een vergelijking van Galois is.**

§ 132. De binomische vergelijkingen van ondeelbaren graad zijn algebraïsch oplosbaar: zij zijn ook inderdaad vergelijkingen van GALOIS.

Is toch gegeven

$$x^p = A$$

waarin A een rationaal getal, geen p^{de}-macht van een rationaal getal is, en is a een der wortels der vergelijking, dan zijn de andere wortels

$$a_1 = \varepsilon\, a,\ a_2 = \varepsilon^2\, a, \ldots .\ \ a_{p-1} = \varepsilon^{p-1}\, a$$

als ε eene complexe p^{de}-machtswortel der eenheid is.

Derhalve:

$$a_i = \frac{a_1^i}{a^{i-1}}\ \ (i = 1, 2, \ldots . p-1).$$

De wortels zijn dus inderdaad rationaal in twee der wortels uit te drukken.

Heeft men ε aan het lichaam der rationale getallen toegevoegd, dan zijn alle wortels in a alleen rationaal uit te drukken: de vergelijking is dan cyclisch geworden.

§ 133. Voor de oplosbare vergelijkingen van deelbaren graad zijn dergelijke algemeene kenmerken niet gevonden. Wij stappen daarom nu van de behandeling van vergelijkingen in 't algemeen af en gaan er ten slotte toe over, aan te wijzen hoe van eene gegeven getallen-vergelijking de algebraïsche oplosbaarheid te onderzoeken is.

In de eerste plaats zal men hebben uit te maken of de vergelijking ontbindbaar is: mocht zij dit zijn, dan is het natuurlijk eenvoudiger, elken onontbindbaren factor afzonderlijk te onderzoeken.

Wil men [1]) rationale factoren $f(x)$ opsporen van de geheele functie $F(x)$ met geheele coëfficiënten, dan kan men vooreerst opmerken, dat, als $F(x)$ van den graad $2n$ of $2n+1$ is, $f(x)$ van niet hoogeren graad dan den n^{den} behoeft ondersteld te worden.

Stellen nu $r_0, r_1, \ldots r_n$ willekeurige geheele positieve of negatieve getallen voor, dan moeten $f(r_0), f(r_1), \ldots$ $f(r_n)$ deelers zijn van $F(r_0), F(r_1), \ldots\ldots F(r_n)$. Maar elke geheele functie $f(x)$ van den n^{den} graad kan in de n^{de}-graadsfunctiën:

$$g_0(x) = \frac{(x-r_1)(x-r_2)\ldots(x-r_n)}{(r_0-r_1)(r_0-r_2)\ldots(r_0-r_n)},$$

$$g_1(x) = \frac{(x-r_0)(x-r_2)\ldots(x-r_n)}{(r_1-r_0)(r_1-r_2)\ldots(r_1-r_n)},$$

. . . .

$$g_n(x) = \frac{(x-r_0)(x-r_1)\ldots(x-r_{n-1})}{(r_n-r_0)(r_n-r_1)\ldots(r_n-r_{n-1})}$$

lineair uitgedrukt worden:

$$f(x) = f(r_0)\,g_0(x) + f(r_1)\,g_1(x) + \ldots + f(r_n)\,g_n(x).$$

Rekent men nu voor een willekeurig stel waarden r_0, $r_1, \ldots r_n$ eerst de functiën $g_0(x), g_1(x), \ldots g_n(x)$ uit, dan zal men voor de coëfficiënten $c_0, c_1, \ldots c_n$ in

$$f(x) = c_0\,g_0(x) + c_1\,g_1(x) + \ldots + c_n\,g_n(x)$$

alleen deelers van $F(r_0), F(r_1), \ldots F(r_n)$ kunnen nemen. Men heeft dus maar voor een eindig aantal stellen coëfficiënten te onderzoeken of $f(x)$ een deeler van $F(x)$ is; zoo kan men dus alle deelers van $F(x)$ vinden of constateeren, dat $F(x)$ onontbindbaar is.

§ 134. Men heeft nu volgens § 89 te vormen de functie

---

[1]) KRONECKER. Grundzüge einer arithmetischen Theorie der algebraïschen Grössen, § 4 bldz. 11.

V der wortels $a, a_1, \ldots a_{m-1}$ der onontbindbare vergelijking $F(x) = 0$:

$$V = \lambda a + \lambda_1 a_1 + \ldots \lambda_{m-1} a_{m-1}$$

deze functie door alle mogelijke substituties over te voeren in $V, V_1, \ldots V_{m!-1}$ en de functie

$$\Phi(\xi) = (\xi - V)(\xi - V_1) \ldots (\xi - V_{m!-1})$$

waarin de coefficienten van de machten van ξ symmetrische functiën der wortels $a, a_1, \ldots a_{m-1}$ en dus uit de coefficienten der vergelijking $F(x) = 0$ te bepalen zijn, op hare ontbindbaarheid te onderzoeken. Neemt men voorloopig voor $\lambda, \lambda_1, \ldots \lambda_{m-1}$ geen bepaalde waarden, dan zijn de coefficienten van de machten van ξ functiën van deze grootheden Maar het onderzoek naar de ontbindbaarheid kan uitgevoerd worden, zooals in de vorige § geschetst is. Vindt men nu een factor van $\Phi(\xi)$, dan ziet men welke grootheden V wortels van deze functie zijn. Zijn dit de grootheden $V, V_a, V_b, \ldots$ dan bevat de GALOIS'sche groep van de vergelijking de substituties $s_0 = 1$, $s_a, s_b, \ldots$

§ 135. Heeft men eenmaal de groep der vergelijking, dan kan men in deze groep alle mogelijke ondergroepen opsporen. Daartoe kan men van elke verzameling substituties, die genomen kan worden, onderzoeken of het product van elke twee in de verzameling voorkomt. Heeft men alle ondergroepen, dan kan men weer nagaan of zij in de groep alleen staan. Zoo kan men dan de samenstellende reeks der groep vormen. Zijn nu de aanwijzers van elke alleenstaande ondergroep in de vorige priemgetallen, dan is de gegeven vergelijking algebraïsch oplosbaar.

De oplossing kan ook uitgevoerd worden, daar het mogelijk is, bij elke alleenstaande groep de daarbij behoorende functie der wortels te vormen en zulk eene functie altijd uit eene cyclische vergelijking gevonden kan worden, die wij boven hebben leeren oplossen.

§ 136. We zien dus, dat het vraagstuk van de algebraïsche oplosbaarheid van eene gegeven getallenvergelijking theoretisch geen moeilijkheden oplevert: practisch is de handelwijze, die zooeven geschetst werd, vrij wel onuitvoerbaar.

De resolvente $\Phi(\xi) = 0$ is van den graad $m!$, d. w. z. bij vergelijkingen van den 3den, 4den, 5den, ... graad is zij van den 6den, 24sten, 120sten, ... graad. Het vormen van deze vergelijking is dus al zeer bezwaarlijk. Bovendien is het onderzoek naar de ontbindbaarheid zeer omslachtig en, heeft men eenmaal de groep der vergelijking gevonden, dan blijft het nog zeer lastig hiervan de ondergroepen en vervolgens de alleenstaande ondergroepen en de samenstellende reeks te bepalen.

Deze handelwijze is dus voor de practische toepassing vrij wel van geen belang. Alleen wanneer men uit den aard van het vraagstuk kan besluiten tot eigenschappen van de groep, die de groep ondubbelzinnig bepalen en hare samenstellende reeks doen kennen, kan men gemakkelijk tot de oplossing der vergelijking komen (zie de vergelijking voor de verdeeling van den cirkel in 17 gelijke deelen, de metacyclische vergelijkingen, enz.).

§ 137. Men kan ook het vraagstuk omkeeren en van de groep uitgaande, daarbij de vergelijking zoeken. Dit heeft F. Hack [1]) gedaan voor de 3de- en 4de-machtsvergelijkingen.

Voor de onontbindbare derde-machtsvergelijkingen, die dus tot groep hebben de symmetrische groep van drie letters

$$s_0 = 1 \qquad s_1 = (a\, a_1\, a_2) \qquad s_2 = (a\, a_2\, a_1)$$
$$s_3 = (a_1\, a_2) \qquad s_4 = (a_0\, a_2) \qquad s_5 = (a_0\, a_1)$$

of haar eenige transitieve ondergroep:

$$s_0 = 1 \qquad s_1 = (a\, a_1\, a_2) \qquad s_2 = (a\, a\;\; a_1)$$

[1]) Dissertatie, Tübingen 1895.

de alterneerende groep, die cyclisch is, is de algebraïsche oplossing, zooals wij reeds gezien hebben, altijd te vinden. HACK gaat na, aan welke voorwaarden de coëfficiënten der vergelijking:

$$x^3 - c_1 x^2 + c_2 x - c_3 = 0$$

moeten voldoen, opdat de vergelijking de cyclische of als men wil, de ABELsche derdemachtsvergelijking zal zijn.

De groep

$$s_0 = 1 \qquad s_1 = (a\, a_1\, a_2) \qquad s_2 = (a\, a_2\, a_1)$$

heeft tot eenige alleenstaande ondergroep de identische met den index ν. Men zal zal dus eene functie van de wortels kunnen kiezen, die uit eene binomische resolvente te vinden is. Neem daarvoor in overeenstemming §§ 113 en 114 de functie van LAGRANGE

$$V = a + \varepsilon a_1 + \varepsilon^2 a_2$$

nadat natuurlijk eerst de complexe derdemachtswortel ε der eenheid aan het lichaam Ω der rationale getallen is toegevoegd, dan zal V^3 eene grootheid van het lichaam $\Omega(\varepsilon)$ zijn en dus

$$V^3 = A + B\varepsilon$$

als A en B getallen van 't lichaam Ω zijn. Daar

$$\varepsilon = \frac{1}{2}(-1 + \sqrt{-3})$$

kan men ook schrijven

$$V^3 = M + N\sqrt{-3}$$

als M en N rationale getallen voorstellen. Maar volgens § 113 wordt dan, als

$$V_1 = a + \varepsilon^2 a_1 + \varepsilon a_2$$

is, voor V_1 gevonden:

$$V_1^3 = A + B\varepsilon^2 = M - N\sqrt{-3}.$$

Hieruit kan men nu uitdrukkingen voor V en V_1 vinden en daaruit zijn in verband met

$$a + a_1 + a_2 = c_1$$

de wortels te bepalen. De vergelijking is dan ook te construeeren.

We merken echter, vóor we daartoe overgaan op, dat $V V_1$ door geen enkele substitutie der groep $s = 1, s_1, s_2$ veranderd wordt; $V V_1$ is dus een getal van Ω, derhalve vindt men

$$M^2 + 3 N^2 = r^3$$

als r een rationaal getal voorstelt. Aan deze voorwaarde hebben de overigens willekeurige rationale getallen M en N te voldoen. N kan bovendien niet nul zijn, want dan zou de vergelijking gelijke wortels hebben.

Denken we, om de verschillende gevallen to onderzoeken, eerst dat $M^3 + 3 N^2 = r^3 = 0$ is, dan moeten M en N noodzakelijk beide van nul verschillen, maar één der factoren $M + N\sqrt{-3}$ of $M - N\sqrt{-3}$ moet nul zijn. $\sqrt{-3}$ behoort dus tot het oorspronkelijke lichaam. V of V_1 wordt in dit geval nul en de vergelijking wordt

$$\left(x - \frac{1}{3}c_1\right)^3 = 2\,M.$$

Zij nu ondersteld:

$$M^2 + 3 N^2 \neq 0,$$

dan kan men $M = m r$, $N = n r$ stellen, waardoor men vindt:

$$r = m^2 + 3n^2, \quad M = m(m^2 + 3n^2), \quad N = n(m^2 + 3n^2)$$

waarin r, m, n rationale getallen zijn.

Men vindt nu:

$$a + a_1 + a_2 = c_1$$

$$V = a + \varepsilon a_1 + \varepsilon^2 a_2 = \sqrt[3]{(m^2 + 3n^2)}\,(m + n\sqrt{-3})$$

$$V_1 = a + \varepsilon^2 a_1 + \varepsilon a_2 = \sqrt[3]{(m^2 + 3n^2)(m - n\sqrt{-3})}.$$

Hieruit volgt (§ 114):

$$a = \frac{1}{3} c_1 + \sqrt[3]{(m^2 + n^2)(m - n\sqrt{-3})} + \\ + \sqrt[3]{(m^2 + n^2)(m + n\sqrt{-3})}$$

$$a_1 = \frac{1}{3} c_1 + \varepsilon \sqrt[3]{(m^2 + n^2)(m - n\sqrt{-3})} + \\ + \varepsilon^2 \sqrt[3]{(m^2 + n^2)(m + n\sqrt{-3})}$$

$$a_2 = \frac{1}{3} c_1 + \varepsilon^2 \sqrt[3]{(m^2 + n^2)(m - n\sqrt{-3})} + \\ + \varepsilon \sqrt[3]{(m^2 + n^2)(m + n\sqrt{-3})}$$

en de vergelijking met deze wortels wordt:

$$x^3 - c_1 x^2 + \left(\frac{1}{3} c_1^2 - 3m^2 - 9n^2\right) x - \\ - (c_1 - 2m)(m^2 + 3n^2) = 0.$$

Elke ABELsche vergelijking van den 3den graad moet in dezen vorm opgesloten liggen: het is echter ook mogelijk, dat de vergelijking in drie rationale factoren to ontbinden is. Dit zal in elk bijzonder geval onderzocht moeten worden. De grootheden m en n moeten daarbij voldoen aan de voorwaarden

$$m \neq 0, \qquad n \neq 0$$

$$m^2 + 3n^2 \neq 0.$$

§ 138. Op dezelfde wijze gaat HACK de vierdemachtsvergelijkingen na. De groepen der onontbindbare vierdemachtsvergelijkingen kunnen, daar zij transitief zijn en hare orde dus door 4 deelbaar is, geen andere zijn dan

1°. de cyclische groep van 4 letters:

$$G_1 = 1, (a\, a_1\, a_2\, a_3), (a\, a_2)(a_1\, a_3), (a\, a_3\, a_2\, a_1).$$

2°. de viergroep

$$G_2 = 1, (a\, a_1)(a_2\, a_3), (a\, a_2)(a_1\, a_3), (a\, a_3)(a_1\, a_2).$$

3°. de groep der 8ste orde

$$G_3 = 1,\ (a_0\,a_2),\ (a_1\,a_3),\ (a\,a_2)(a_1\,a_3),$$
$$(a\,a_1)(a_2\,a_3),\ (a\,a_3)(a_1\,a_2),\ (a\,a_1\,a_2\,a_3),\ (a\,a_3\,a_2\,a_1).$$

Dit is de ondergroep g_1 van § 49.

4°. de alterneerende groep van 4 letters:

$$G_4 = 1,\ (a\,a_1)(a_2\,a_3),\ (a\,a_2)(a_1\,a_3),\ (a\,a_3)(a_1\,a_2),$$
$$(a\,a_1\,a_2),\ (a\,a_1\,a_3),\ (a\,a_2\,a_1),\ (a\,a_2\,a_3),$$
$$(a\,a_3\,a_1),\ (a\,a_3\,a_2),\ (a_1\,a_2\,a_3),\ (a_1\,a_3\,a_2).$$

5°. de symmetrische groep G van 4 letters.

§ 139. In het eerste geval is

$$1,\ (a\,a_2)(a_1\,a_3)$$

eene alleenstaande ondergroep van index 2 van G_1. De functie $(a - a_1)(a_2 - a_3)$, die hierbij behoort, kan dus uit eene vierkantsvergelijking gevonden worden. Is dus p rationaal en $\sqrt{p}$ niet, dan vindt men

$$(a - a_1)(a_2 - a_3) = 4\sqrt{p}. \qquad (1)$$

Voegt men deze grootheid aan het lichaam Ω toe, dan reduceert zich de groep tot bovenstaande ondergroep van 2 substituties. Voor de functie V, die voor deze 2 substituties verschillende waarden krijgt zou men kunnen nemen

$$V = a + a_1 - a_2 - a_3$$

waardoor men zou vinden

$$V_1 = a_2 + a_3 - a - a_1 = -V.$$

Daardoor zou in 't lichaam $\Omega\,(\sqrt{p})$ de functie V^2 rationaal worden en wel $V^2 = l + m\sqrt{p}$.

Men zou nu, daar $(a-a_1)(a_2-a_3)$ en $(a-a_1) + (a_2-a_3)$ bekend zijn, $a-a_1$ en $a_2 - a_3$ afzonderlijk kunnen vinden en vervolgens ook a, a_1, a_2 en a_3.

HACK doet het eenigszins anders: hij merkt op, dat

$$(a-a_2)^2 + (a_1-a_3)^2$$

door geen substitutie van G_1 verandert en dus tot het lichaam Ω behoort en stelt:

$$(a-a_2)^2 + (a_1-a_3)^2 = 8\,q. \qquad (2)$$

Verder wijst hij er op, dat

$$\frac{(a-a_2)^2 - (a_1-a_3)^2}{(a-a_1)\,(a_2-a_3)}$$

onveranderd blijft voor alle substituties van G_1 en dus tot het lichaam Ω behoort; dat derhalve

$$(a-a_2)^2 - (a_1-a_3)^2 = 8\,r\sqrt{p} \qquad (3)$$

kan gesteld worden. Maar dan voldoen p, q en r aan de vergelijking

$$q^2 = p\,(1 + r^2) \qquad (4)$$

Daaruit blijkt, dat $1 + r^2$ geen kwadraatgetal mag zijn. Uit (2) en (3) volgt nu

$$a - a_2 = 2\sqrt{q + r\sqrt{p}} \text{ en } a_1 - a_3 = 2\sqrt{q - r\sqrt{p}}$$

Uit

$$a + a_1 + a_2 + a_3 = c_1$$

en

$$a + a_2 - a_1 - a_3 = 4\,s\sqrt{p}$$

waarin s rationaal is omdat $\dfrac{a + a_2 - a_1 - a_3}{(a - a_1)\,(a_2 - a_3)}$ bij de groep G_1 behoort, vindt men nu

$$a + a_2 = \frac{1}{2}\,c_1 + 2\,s\sqrt{p} \text{ en } a_1 + a_3 = \frac{1}{2}\,c_1 - 2\,s\sqrt{p}$$

Zoo komt men eindelijk tot de wortels:

$$a = \frac{1}{4}\,c_1 + s\sqrt{p} + \sqrt{q + r\sqrt{p}}$$

$$a = \frac{1}{4}\,c_1 - s\sqrt{p} + \sqrt{q - r\sqrt{p}}$$

$$a = \frac{1}{4} c_1 + s \sqrt{p} - \sqrt{q + r\sqrt{p}}$$

$$a = \frac{1}{4} c_1 - s \sqrt{p} - \sqrt{q - r\sqrt{p}}$$

Nu kan men de vergelijking, die G_1 tot groep heeft opstellen. Verdrijft men daarin den 2den term, d. w. z. stelt men $c_1 = 0$, dan vindt men

$$y^4 - 2(ps^2 + q)y^2 - 4prsy + s^4 - 2pqs^2 + p = 0$$

als type der Abelsche vergelijkingen van den 4den graad, die de groep G_1 tot groep hebben. De grootheden p, q, r, s moeten hierin voldoen aan de voorwaarden

$$p \neq 0, \qquad q^2 = p(1 + r^2)$$

terwijl p en $1 + r^2$ geen kwadraatgetallen mogen zijn.

§ 140. Op dergelijke wijze gaat Hack de andere groepen na.

Hij vindt voor de vergelijking in het 2de geval

$$y^4 - 2(p + q + r^2pq)y^2 - 8rpqy +$$
$$+ (p - q)^2 + r^2pq(r^2pq - 2p - 2q) = 0$$

waarin p en q niet nul en geen kwadraatgetal mogen zijn en ook pq geen volkomen vierkant mag wezen.

In het 3de geval vindt hij voor de vergelijking

$$y^4 - 2(r^2q + p)y^2 - 4rqy + (r^2q - p)^2 - q = 0$$

waarin q, $p^2 - q$ en $\frac{p^2}{q} - 1$ noch nul, noch een volkomen vierkant mogen zijn.

Eindelijk in 't 4de geval vindt hij

$$y^4 - 6py^2 + 8qy + 12(m^2 + 3n^2) - 3p^2 = 0.$$

§ 141. Cayley heeft op dergelijke wijze bepaald de gedaante van de algebraïsch oplosbare vijfdemachtsvergelijkingen [1]); wij zullen hier niet op ingaan. Een enkele

[1]) Collected mathematical papers, vol. V, bldz. 55; Phil. Mag. vol XXI, bldz. 257.

blik op de formule, waartoe CAYLEY komt en die, voluit geschreven, zeker niet op ééne bladzijde van dit proefschrift plaats zou kunnen vinden, is voldoende om te doen zien, dat men ook met groote bezwaren te strijden heeft, als men de kennis van de algebraïsche oplosbaarheid van bepaalde numerieke vergelijkingen langs dezen weg verder wil brengen.

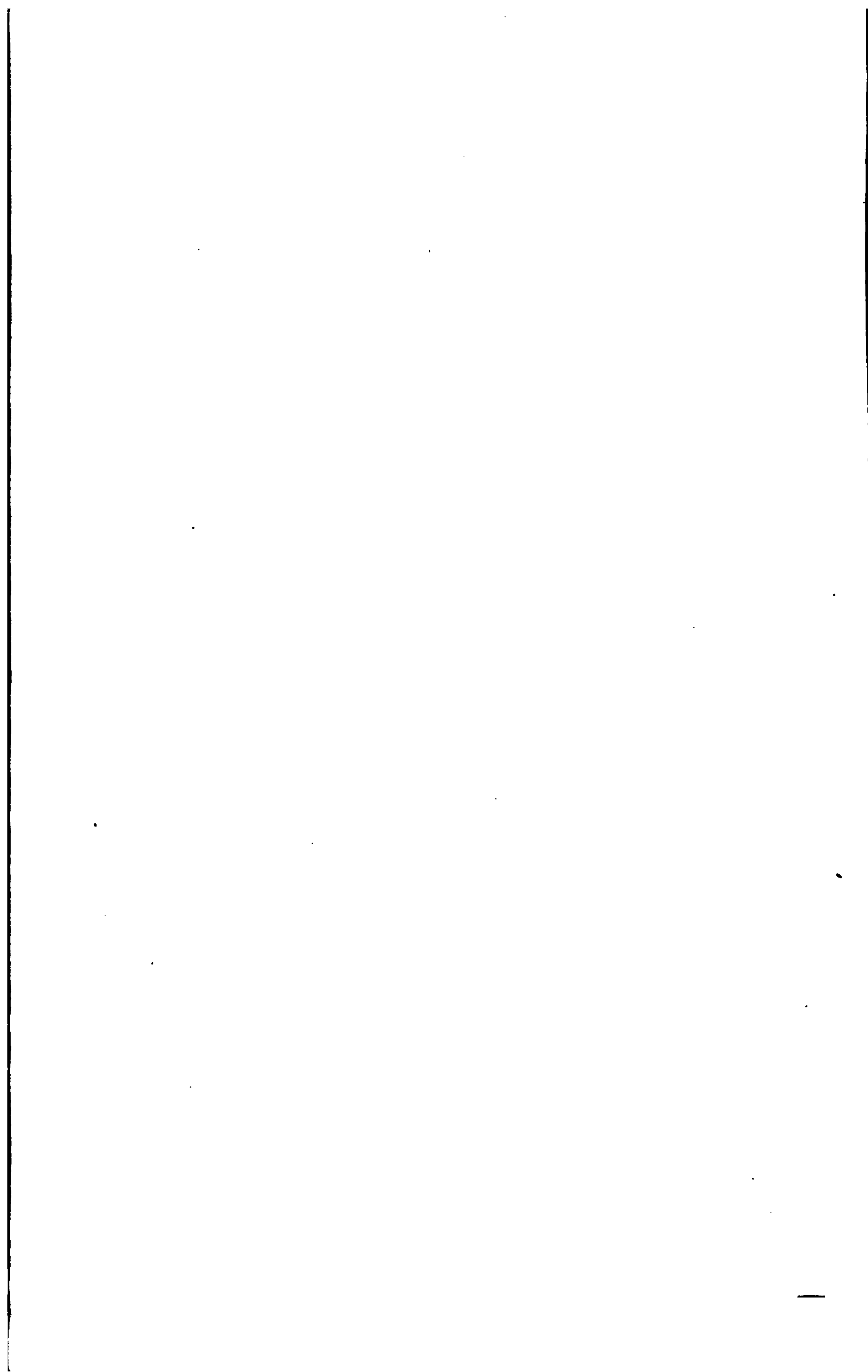
§ 142. Daarbij komt nog een andere moeilijkheid: als men deze handelwijze wil toepassen op vergelijkingen van ondeelbaren graad, kent men ten minste de groepen, van welke men moet uitgaan: het zijn de metacyclische groep en transitieve ondergroepen daarvan. Voor de vergelijkingen van deelbaren graad zijn echter alleen in bijzondere gevallen groepen onderzocht, die als groep van de vergelijking in aanmerking kunnen komen: van de *oplosbare* groepen van deelbaren graad, d. w. z. de groepen van deelbaren graad, welker samenstellingsfactoren priemgetallen zijn, is tot nu toe geen algemeene vorm gevonden.

HÖLDER [1]), FROBENIUS [2]), BURNSIDE [3]) hebben wel verschillende oplosbare groepen van meer of minder algemeenen vorm gegeven, maar overigens leidt de theorie der substitutiegroepen in haar tegenwoordige ontwikkeling ons nog niet tot de kennis van de algemeene gedaante van de groepen der algebraïsch oplosbare onontbindbare vergelijkingen van deelbaren graad.

Voor de vergelijkingen van priemgraad hebben de stellingen van GALOIS het vraagstuk geheel opgelost.

---

[1]) Mathematische Annalen, XL. [2]) Berl. Sitzungsber. 1895.
[3]) Proc. London Math. Soc. XXVI.



STELLINGEN.

I.

Het kriterium van GALOIS voor de algebraïsche oplosbaarheid van hoogere-machtsvergelijkingen is tot nu toe practisch onbruikbaar, wanneer uitgemaakt moet worden of eene hoogere-machtsvergelijking met gegeven getallencoëfficienten al of niet oplosbaar is door wortelgrootheden.

II.

Niet CAUCHY maar RUFFINI is te beschouwen als de grondlegger van de theorie der substitutiegroepen.

III.

WEBER's formuleering van de „Stelling van ABEL":

> Jede mögliche Reduction der GALOIS'schen Gruppe wird herbeigeführt durch Adjunction einer natürlichen Irrationalität . . . . [1])

is onjuist.

IV.

Het bewijs voor de onontbindbaarheid van de vergelijking voor de verdeeling van den cirkel in een ondeel-

[1]) WEBER. Algebra, 1e Auflage. Bnd. I, Blz. 516.

baar aantal gelijke deelen, dat men vindt bij NETTO [1]), is onvolledig.

V.

De onderverdeeling van de groepentheorie, die men vindt onder J 4 in den „Index du réportoire bibliographique des sciences mathématiques" is onlogisch.

VI.

Het gebruik van den naam „nevengroep" voor de rijen substituties (α), (β), ... van § 44 is af te keuren [2]).

VII.

Bij eene wetenschappelijke behandeling van de grondslagen der meetkunde is het wenschelijk af te zien van de axioma's en de bepalingen in den Ecclidischen vorm en als uitgangspunt te kiezen de grondeigenschappen van de continue groepen.

VIII.

Het is wenschelijk de begrippen „operatiesymbool" en „grootheid" scherper te scheiden dan dikwijls gedaan wordt.

IX.

De kwikzilver-calomel-elektrode in $^1/_{10}$ N.-chloorkaliumoplossing verdient als normaalelectrode de voorkeur boven de waterstofelectrode in normaal zuur.

---

[1]) NETTO. Substitutionentheorie. Bldz. 174.

[2]) WEBER. § 154. KIRKMAN. Mem. of the lit. and phil. Society of Manchester, Serie 3, Vol. I, Bldz. 274.

X.

Het onderwijs in de natuurkunde aan de Hoogere Burgerscholen met vijfjarigen cursus wordt veel te hoog opgevoerd.

XI.

Het is niet wenschelijk, den moleculairen druk op een vlakte-element te definieeren als de kracht, waarmee alle stof aan den eenen kant van het platte vlak, waarin het element gelegen is, het stoffelijk zuiltje met dat element tot grondvlak, aan den anderen kant van het vlak gelegen en loodrecht hierop rustend, aantrekt in de richting normaal op dit vlak. [1])

XII.

Ten onrechte zegt prof. G. HEYMANS [2]):

> . . . . Nach alledem wäre also das Trägheitsprincip nicht ein empirisches Gesetz und auch nicht ein apriorisches Axiom, sondern eine Schlussfolgerung aus empirischen und apriorischen Daten . . . . . .
>
> . . . . . . die aussergewöhnliche Gewissheit [desselben] sowie die Beziehung desselben auf absolute Bewegung [ist] der Mitwirkung apriorischer Daten zu verdanken.

XIII.

De onjuistheid van prof. BOLLAND's uitingen [3]) over irrationale getallen vindt zijn oorzaak in eene te beperkte opvatting van het getalbegrip.

---

[1]) H. HULSHOF. Dissertatie Amsterdam, 1900, bldz. 37.

[2]) Die Gesetze und Elemente des Wissenschaftlichen Denkens, 1894, 2ter Band. Blz. 438.

[3]) Aanschouwing en verstand. Leiden 1897.